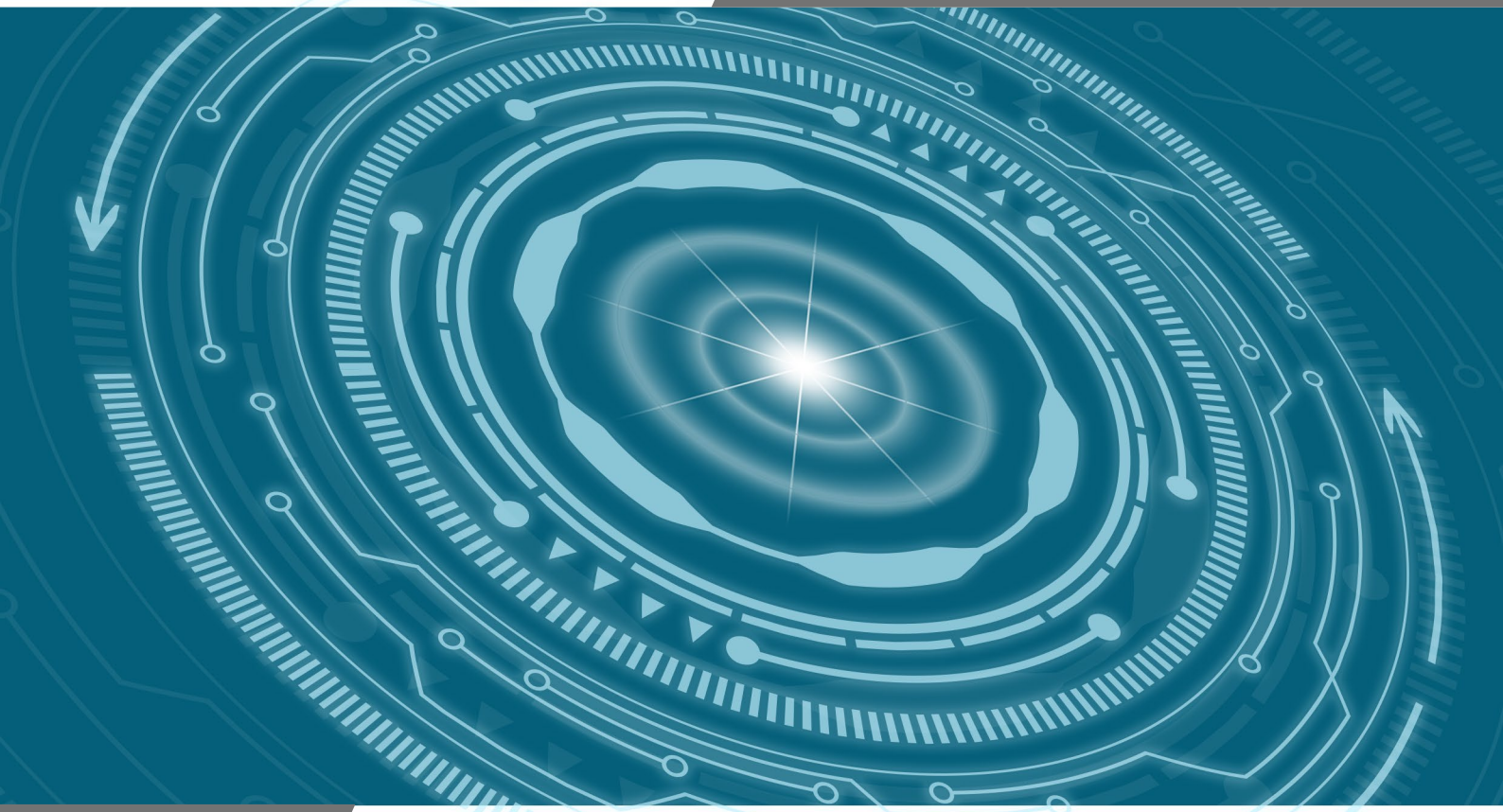
Ekonomi ve Dış Politika Araştırmalar Merkezi

edam

Siber Politikalar ve Dijital Demokrasi 2018/4



Mayıs 2018

Dijital Gözetleme, Milli Güvenlik ve Özel Hayatın Gizliliği Siyaseti

H. Akın Ünver | EDAM, Oxford CTGA & Kadir Has Üniversitesi

Dijital Gözetleme, Milli Güvenlik ve Özel Hayatın Gizliliği Siyaseti

H. Akın Ünver | EDAM, Oxford CTGA & Kadir Has Üniversitesi

Yönetici Özeti:

Snowden ifşaatlarının, daha sonraki milli güvenlik sızıntılarının ve son olarak Cambridge Analytica ve Trump kampanyası ile ilgili ihtilafın ardından, dijital gözetleme gittikçe büyüyen küresel bir endişe haline gelmiştir. Bu raporda dijital gözetleme ile ilgili bazı ikilemler ve açmazlar, demokrasiler ve otokrasilerdeki kapsamı ve SIC olarak bilinen 'gözetleme-sınai kompleksi' ile nasıl etkileşime girdiği incelenmektedir. SIC, gözetlemeyi sorunlu kılan amaçları değil de iş modeli olduğundan, gözetleme-özel hayatın gizliliği tartışmasında sıklıkla göz ardı edilmektedir. Tüm siyasi sistemlerde, bir ülkenin sırları (vatandaş verileri, uluslararası veri transferleri) toplama ya da meşruiyet adına bazı anahtar siyasi bilgileri halka ifşa etme istekliliğine yön veren bir gizlilik, şeffaflık ve gözetleme maliyeti vardır. Dijital uzaydaki gözetleme-özel hayatın gizliliği tartışmasının temel bir bileşeni, devletlerin - ağlar ile birbirlerine bağlı bir toplumda temel istihbaratları elde etmenin giderek artan maliyetleri nedeniyle - politika bilgilerini ifşa etmedeki isteksizliğine yön veren teknoloji yarışıdır. Sayıları gittikçe artan gözetleme ve aynı şekilde atlatma yöntemleri ve teknolojileri, gözetleme mekanizmalarını düzenlemeye ve korumaya yönelik çabaların başarısız olmasının asıl nedenlerinden birisidir: bunlar, teknolojik açıdan yetkin istihbarat kurumlarına ya da her zamankinden daha becerikli vatandaş-güdümlü atlatma araçlarına ayak uyduramamaktadır. Bazı Avrupa ülkelerindeki iyi örnekler, bürokratlara ya da parlamenterlere ek olarak yetkin teknik uzmanlar tarafından oluşturulan melez koruma mekanizmaları geliştirilmesiyle, daha çok gözetleme denetiminin şeffaf hale getirilmesine odaklanmaktadır. Gözetleme şeffaflığı hareketlerinin başarısızlığı büyük ölçüde koruma ve denetim mekanizmalarının bu teknolojik geriliğinden kaynaklanmaktadır; bunun sonucunda halk devletlerin dijital istihbaratı ve vatandaş verilerini yönetme ve işleme şeklini atlatmaya, maskelemeye ya da izlemeye yönelik kendi mekanizmalarını geliştirmektedir. Bununla birlikte özellikle artan terör tehdidi, aşırı sağ radikalleşme ve batı toplumlarında ortaya çıkan aşırı gruplar ile birlikte, gözetleme sadece siyasi olarak gerekli değil, aynı zamanda seçimler açısından halka hitap eden bir husus olarak görülmektedir. Bu açıdan kamuoyu tek bir görüşte değildir; kendi içinde gözetlemeyi savunan ve özel hayatın gizliliğini savunan gruplar arasında bölünmüştür. Sonuç olarak, demokrasilerin ülkenin siyasi kültürüne, ancak aynı zamanda evrensel insan haklarına uyan bir gözetleme-özel hayatın gizliliği dengesi kurmaları gereklidir. Bu bağlamda denetim görevi ağır bir görevdir: suistimalleri ve aşırılıkları tespit etmek için yürütme ve istihbarat toplumunu sürekli olarak takip etmesi ve aynı zamanda teknolojik açıdan yetkin kalması gerekmektedir.

Bu araştırma ABD merkezli Chrest Vakfı'nın fon katkısı ile gerçekleştirilmiştir.

Giriş

2018 Mart ayının ortasında, veri danışmanlık şirketi Cambridge Analytica'nın Trump kampanyası ile hukuk dışı ilişkileri ifşa edildi; şirket, kullanıcıların izni ve yasal gerekçe olmaksızın 50 milyondan fazla Facebook profilini toplamıştı. Bu profiller daha sonra psikolojik profiller olarak kataloglanmış ve Analytica'nın Facebook kullanıcılarının haber kaynağındaki haber sonuçlarını çarpıtan bir algoritma oluşturmasına olanak vermişti. Eleştirilere göre bu sadece yasa dışı değildi, aynı zamanda ABD seçim kampanyasını sonucunu önemli ölçüde etkilemişti. Cambridge Analytica CEO'su Alexander Nix, o zamanlar Trump kampanyasındaki önde gelen isimlerden biri olan ve daha sonra kısa bir süreliğine de olsa Amerika Birleşik Devletleri Başkan Yardımcılığı görevini yürüten Steve Bannon ile doğrudan bağlantılıydı. Facebook, 50 milyon profilin ham verilerini kıdemli bir Analytica veri bilimcisi olan Aleksandr Kogan'a isteyerek ifşa ederek skandalda aktif bir aktör olarak rol almıştı. Kogan, Facebook'taki bir anket uygulaması olan 'thisismydigitallife' adlı uygulamayı geliştirmiş ve bu uygulama da söz konusu verilerin siyasi bir kampanyada kullanılacağını bilmeden ankete yanıt veren ilk 270.000 Facebook kullanıcısının profillerini çıkarmıştı.[1] Kogan, ağ analiz yöntemleri (arkadaşlar, ilgi alanları, beğeniler) sayesinde bu ilk 270.000 kullanıcı yoluyla 50 milyon kullanıcının verilerine erişebilmişti. Bu skandal siyaset - gözetleme - teknoloji endüstrisi rabıtasındaki yoğun güç ilişkilerini ortaya koyarak kişisel verilerin güvenliği, veri paylaşma, veri koruma ve veri yerelleştirme açısından dijital dünyaya bir uyarı sinyali göndermişti.

İhtilaflı bir terim olan dijital gözetleme, çevrim-içi ayak izinin - söz konusu verilerin ait olduğu aktörün (aktörlerin) iradesi ve/veya bilgisi dışında - gerçek zamanlı ve geçmişe dönük görüntülenmesi, işlenmesi ve kataloglanması olarak geniş kapsamlı bir şekilde tanımlanabilir.[2] Tartışmanın merkezinde, verileri gözetlenen aktörün (aktörlerin) rızası ile bilgisi ve söz konusu izleme eyleminden elde edilen emniyet, bilgi ve istihbarat faydaları yer almaktadır. Öte yandan özel hayatın gizliliği, izinsiz müdahaleye uğramama özgürlüğü şeklinde daha dolambaçsız bir tanıma sahiptir.[3] Bu kavramlar ve bunların etrafındaki tartışmalar yeni olmamakla birlikte, karşılıklı dijital bağlantılılığın ortaya çıkışı, sosyal medya ve dijital aktörlerin kişisel bilgileri yayabileceği ve ifşa edebileceği diğer kanallardaki önemli artış, tartışmanın ölçüsünü önemli derecede değiştirmiştir. Hızla değişen bağlantı teknolojileri, dijitalleştirilmiş kişisel bilgilerin ve resmi verilerin artık bir çok noktadan ele geçirilebileceği, güvenli bir biçimde silinemeyeceği, geçerliliğini yitirmeyeceği ve sonsuz bir oranda ve baş döndürücü bir hızla dijital platformlar genelinde yayılabileceği bir sistem yaratmaktadır.

Gözetlemenin etiği ve felsefesi hakkındaki mevcut tartışma, büyük ölçüde Jeremy Bentham'ın 'panoptikon'[4] ve Michel Foucault'nun 'panoptisizm'[5] kavramlarından türemiştir. Panopticon idealleştirilmiş, maliyet-etkin, 18nci yüzyıl sonu bir hapishane mimari modeliydi; bu model tüm mahkumları görebilen ancak mahkumların izlenip izlenmediklerini göremedikleri tek, merkezi, gizlenmiş bir gözetleme kulesinden oluşmaktaydı. Baş gardiyan gizlenmiş olduğundan ve mahkumların ne zaman izlendiklerini ya da hiç izlenip izlenmediklerini kestirmeleri imkansız olduğundan, sistem kolektif bir korku ve sürekli izlenme psikolojisine dayanmaktaydı. Panoptikon kavramının, Michel Foucault'nun otoriterizm ve gözetleme konusundaki eserleri üzerinde büyük bir etkisi olmuştur; Foucault bu eserlerinde, görülmeden ya da izlenmeden bireylerin hayatlarına girme ve müdahale etme yetisinin bir güç mekanizması ve bir kontrol kültürü yarattığı modern 'disiplin toplumlarını' tanımlamak için 'panoptisizm' terimini kullanmıştır. Panoptikon mimarisinin disipline edici gücü karmaşık kilitlere, parmaklıklara ya da gardiyanlara değil, (açık ve görünür gözetleme yerine) görünmez gözetleme tehdidine dayanmaktadır. Panoptikonun benzer eleştirel yorumları, panoptikonu yeknesak kolektif davranışı pekiştiren ve sıkı kültürel davranış modlarından sapmanın sosyal maliyetlerini arttıran bir baskı ve sosyal kontrol aracı olarak tanımlayan Gertrude Himmelfarb[6] ve Jacques-Alain Miller'in[7] eserlerinde de mevcuttur. Bu açıdan, panoptikon ve panoptisizm devlet kontrolünün ve sosyal örgütlenmenin otoriter modları olarak görülebilir, ancak Foucault'nun eleştirisi, otoriter devletlerin müdahaleci niteliklerinin ötesine geçmektedir. Faucault, demokratik ülkelerdeki sosyal güçlünün yanında olma eğilimlerini ve bir komünün - devlet gerçekte ne kadar müdahaleci olursa olsun kontrol edile-

[1] Alvin Chang, "The Facebook and Cambridge Analytica Scandal, Explained with a Simple Diagram," Vox, 23 Mart 2018, https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram.

[2] Marx Gary T., "A Tack in the Shoe: Neutralizing and Resisting the New Surveillance," Journal of Social Issues 59, no. 2 (29 Nisan 2003): 369–90, https://doi.org/10.1111/1540-4560.00069; Andrew Chadwick and Philip N. Howard, Routledge Handbook of Internet Politics (Taylor & Francis, 2010).

[3] Sabrina De Capitani Di Vimercati ve ark., "Data Privacy: Definitions and Techniques," International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 20, no. 6 (1 Aralık 2012): 793–817, https://doi.org/10.1142/S0218488512400247.

[4] Jeremy Bentham, Panopticon: The Inspection House (CreateSpace Independent Publishing Platform, 2017).

[5] Michel Foucault, Discipline & Punish: The Birth of the Prison, çeviren Alan Sheridan (New York: Vintage Books, 1995).

[6] Gertrude Himmelfarb, The Roads to Modernity: The British, French, and American Enlightenments, Yeni basım (New York New York: Vintage, 2005).

[7] Jacques-Alain Miller ve Richard Miller, "Jeremy Bentham's Panoptic Device," Ekim 41 (1987): 3–29, https://doi.org/10.2307/778327.

meyecek duruma gelerek - birbirinin aleyhine dönme ve panoptikonun müdahaleci niteliklerini pekiştirme eğilimini eşit derecede eleştirmektedir.

Gerçekten de bazı kişiler yeni gözetim yöntemlerinden ve araçlarından asıl yararlananların devletler olduğunu savunmaktadır. 2010-2013 Arap Baharı ve Occupy (İşgal Et) hareketlerinin ilk şokunun (ve bunlardan alınan derslerin) ardından kendilerini toparlayan çoğu devlet, sosyal medya güdümlü protestolar ve dijital mobilizasyon yöntemleri çağına kendilerini adapte etmiştir. Örneğin Çin'in- bir dizi filtreleme ve izleme mekanizması için kullanılan şemsiye bir terim olan- 'Büyük Ateş Seddi, kullanıcı girişlerini ve anahtar sözcüklerini izlemek için Derin Paket İncelemesini (DPI) kullanabilmekte, sosyal hareketleri ve mobilizasyon örüntülerini tespit etmek için yapay zeka kullanmaktadır. Çin ayrıca yakın zamanda kolluk amaçları için vatandaşların gerçek zamanlı yüz tanıma analizini yapan polis gözlüklerini ortaya çıkarmıştır. Rusya, yetki gerekmeden analog ve elektronik haberleşmelerin tamamen gözlenmesine olanak veren SORM'ye (İşlemsel Araştırma Faaliyetleri Sistemi) sahiptir. Amerika Birleşik Devletleri ve Avrupa Birliği devletleri, istihbarat ve emniyet amaçlarına yönelik olarak farklı derecelerde ağ izleme, yığınsal veri analizi, derleme ve gerçek zamanlı kataloglama faaliyetleri yürütmektedir.

Demokrasiler ve otoriter devletler, hukuki ve yasama ile ilgili koruma tedbirleri farklı düzeylerde olsa da, birbirlerine benzer şekilde geniş kapsamlı kitle gözetim uygulamaları yürütmekte ve çoğu kez benzer araçlar kullanmaktadır. Teknoloji, geniş devlet kaynakları ve olanakları ile birleştiğinde, sağlık verilerinden tüketim davranışlarına ve seçmen davranışlarına kadar tarihsel olarak eşi görülmemiş hacimlerde ve öge boyutunda vatandaş bilgilerine erişime sahip küresel 'elektronik polis devletlerinin' ortaya çıkmasına yol açmıştır; devletlerin çoğu cep telefonu meta-verilerini toplayıp işleyebilmekte ya da bireyleri gerçek zamanlı izlemek için doğrudan cep telefonu izlemeyi kullanmaktadır. Milli güvenlik ve terörle mücadele amaçları için kullanıldığında dahi, toplanan kitlesel vatandaş verilerinin ölçeği ve ayrıntıları bireysel özgürlükler ve özel hayatın gizliliğine ilişkin haklı olarak kötümser gözlemlere yol açmaktadır. Oxford İnternet Enstitüsünde Araştırma Yöneticisi olan Philip Howard'ın sözleriyle: 'bizler, vatandaş olarak, birinci özel hayatın gizliliği savaşını kaybettik'.[8]

Bununla birlikte, özel hayatın gizliliği savaşını kaybedenler sadece vatandaşlar değildir. Tüketicilere yönelik insansız hava araçlarının yaygınlaşması ve yüksek çözünürlüklü tüketici uydu görüntülerinin kitlesel bulunabilirliği, vatandaşların uzak yerlerdeki askeri üslerin ve tesislerin yerlerini belirlemelerine ve bunları izlemelerine olanak vermektedir. Sosyal medyadaki çatışma izleyiciler, çatışma bölgesinde bulunan kişilerden bilgi, görüntü ve video derleyip düzenlemekte ve bunları devlet propagandasını ve bilgi kanallarını baypas ederek coğrafi konum, tarih ve saat ile bildirebilmektedir. Bellingcat gibi açık kaynaklı matematiksel analiz inisiyatiflerinin yaygınlaşması ile halka açık veri kaynakları 'dijital adli tıp' işlemleri yapmak için kullanılabilmekte ve MH-17 uçuşunun Ruslar tarafından düşürülmesi, Rus birliklerinin Kırım'daki varlığı gibi son derece hassas askeri konular, bu konular resmi kanallardan duyurulmadan çok önce keşfedilmektedir.[9] Bunlara ek olarak, söz konusu kaynaklar Suriye'deki sarin gazı saldırılarını belgeleyen ve kanıt sunan ilk kaynaklardır. Kısa süre önce, koşuculara yönelik bir mobil uygulama ve sosyal ağ kurma sitesi olan Strava, kaydedilen koşunun güzergahını, rakımını, hızını, zamanını ve coğrafi konumunu içeren kullanıcı verilerini halkın görüntülemesine ve arama yapmasına açmıştır. Kısa süre sonra birçok kullanıcı arama yapılabilen ısı haritası verileri yoluyla dünya üzerinde açıklanmayan yerlerde bulunan gizli A.B.D. üslerini ve diğer askeri üsleri tanımlamış ve dünya genelinde bu tür bazı askeri tesisleri ve ileri konuşlandırma mevzilerini ifşa etmiş ve tehlikeye düşürmüştür.[10]

Bu açıdan, 'birinci özel hayatın gizliliği savaşını' kaybedenler sadece vatandaşlar değildir; vatandaşlar gibi devletler de bu ilk savaşın kaybedenleri arasındadır. Teknoloji şirketleri, gözetleme teknolojisi tedarikçileri ya da İnternet Servis Sağlayıcıları gibi bu tür verileri toplayanlar ve biriktirenler de sözcüğün gerçek anlamıyla aslında 'kazanmış' değillerdir. Yeni devlet sırrı ve özel veri toplama ve yayma türlerinin ortaya çıkarılması, bu şirketler üzerindeki yasama, kanun ve demokratik denetim baskılarının artmasına yol açmış ve bu şirketleri dünyanın en gergin diplomatik ve sosyal krizlerinin bazılarında rol alan siyasi oyuncular haline getirmiştir. 'Birinci özel hayatın gizliliği savaşının' sonunda gerçekten baskın gelen, Foucault'nun 'panoptisizm' sorunu, yani gözetleme kültürünün kendisi ve sürekli izlenme korkusu ve bunun yol açtığı infial olmuştur. Bu genel dijital korku ve karşılıklı infial halinde, devletler, vatandaşlar ve şirketler gözetlemenin farklı yönlerine karşı aynı şekilde savunmasızdır. Bu durum siyasi, ekonomik ve sosyal nitelikli küresel, bölgesel ve ulusal sonuçları olan ve tüm tarafları kendi ifade özgürlüklerini sınırlamaya ve oto-sansüre zorlayan bir dijital yönetim kördüğümü doğurmaktadır.

8 'Sosyal Medya Demokrasiyi Öldürüyor Mu' adlı bu açılış dersinin Prezi versiyonuna aşağıdaki adresten erişilebilir: https://prezi.com/cxuukuoovaoc/is-social-media-killing-democracy/

9 MH17 – Açık Kaynaklı Araştırma, Üç Yıl Sonra: https://www.bellingcat.com/news/uk-and-europe/2017/07/17/mh17-open-source-investigation-three-years-later/

10 Alex Hern, "Strava Suggests Military Users 'Opt Out' of Heatmap as Row Deepens," the Guardian, 29 Ocak 2018, http://www.theguardian.com/technology/2018/jan/29/strava-secret-army-base-locations-heatmap-public-users-military-ban.

Gözetleme-Milli Güvenlik Bağlantısı

Serbest bilgi akışı uzun zamandır demokrasilerin ayırıcı özelliği olarak kabul edilmektedir. Almanya ve Pakistan vatandaşlarının kendi devlet bilgilerine ya da siyasi süreçlere eşit erişime sahip olmamalarının ardındaki neden, bu iki ülkenin farklı rejim türlerine sahip olmalarının başlıca nedenlerinden biridir. Ancak bu, halkın siyasi bilgilere erişiminin tüm demokrasilerde aynı olduğu anlamına gelmez; aradaki karşıtlık dijital haberleşme devriminden bu yana daha da belirgin hale gelmiştir. Modern demokrasilerde, ülke dışındaki çeşitli milli güvenlik operasyonlarını ve menfaatlerini korumak için gerekli 'meşru gizlilik' kavramı için farklı ve çoğu kez çelişen yorumlar vardır. Siyaset bilimci Michael Colaresi, gizliliğin tüm kullanımlarının ve suistimallerinin, devletlerin belirli hacimde bilgiyi gizli kılabilmek için harcaması gereken bir 'gizlilik maliyeti' gerektirdiğini savunmaktadır.[11] Bu maliyetler arasında şifreleme, sırları depolamak için gerekli fiziksel altyapı ile bu bilgi kümelerini düşmanının ellerinin yanı sıra halkın gözünden uzak tutmak için gerekli karmaşık güç ilişkileri (kolluk kuvvetleri, istihbarat aygıtı, vb.) vardır. Bu maliyetler genellikle stratejik kullanımlarına göre harcanır: düşman hareketlerini kestirmek, düşmanları aldatmak ve kriz dönemleri sırasında rakip kabiliyetleri bastırmak için. Bir devlet - altyapı, kriptografi, kurumsal-örgütsel kapasite ya da insan niteliği açısından - gizliliğe ne kadar fazla harcama yaparsa, rakip devletlerin dikkatini o kadar iyi başka yöne çekebilir, yanlış yönlendirebilir ve bunlara karşı stratejik üstünlük elde edebilir.

Öte yandan, gizlilik maliyetlerinin seçmen maliyetleri ile çeliştiği yegane rejim türü, demokrasilerdir. Sadece demokrasilerde, gizliliğe harcanan her bir birim maliyet için halktan kaynaklanan - devletin gizli tutmaya çalıştığı bilgi türünün şeffaflığını isteyen - başka bir karşı güç vardır. Liderleri gizlilik gücünü suistimal etmekten caydıracak süreci kim denetleyecektir? Sivil toplum ve parlamento, karar vericileri politika seçimlerinden dolayı sorumlu tutmaya yönelik esas görevini nasıl yerine getirecektir? Gizlilik, düşmanı yanlış yönlendirmek ve sindirmek için kullanıldığı gibi, aynısını halka ya da denetim kurumlarına yapmak için de kolayca kullanılabilir. Siyaset bilimci Michael Desch'e göre, demokrasilerin ve otoriter ülkelerin gizliliği ve gözetlemeyi ele alma şekilleri son derece benzerdir, ancak demokrasilerde en büyük farkı oluşturan hususlar seçmen maliyetleri ve politika cezasıdır. Bir demokraside, liderlerin gizliliği ve gözetlemeyi yönlendirmelerine yönelik kısıtlamalar, bu sırları halktan (ve düşman gözlerden) tecrit eden ve aynı zamanda bu tür bilgilerin ele alınmasına yönelik şüpheler olduğunda halkın hükümete baskı yapmasına olanak veren birbirleri ile bağlantılı karmaşık bir katmanlar kümesi yoluyla kurumsallaştırılmıştır. Bu açıdan demokrasilerde, söz konusu devletlerin belirli sırları halkın bilgisine açmaları için ödemeleri gereken bir 'şeffaflık maliyeti' de vardır. Hükümetin demokratik amaçlarla halka açıkladığı her sırrın otomatik olarak düşmanla da paylaşılması bakımından, şeffaflık maliyetleri gizlilik maliyetleri ile etkileşim halindedir. Bu tür hareketlerin şeffaflık maliyetlerini dengelemek için, devletin yeni bilgileri sır haline getirmek için daha da fazla yatırım yapması gereklidir, aksi halde rakip devletlere karşı temel karşılaştırmalı üstünlüğünü kaybedecektir.

Bununla birlikte tüm sırlar milli güvenlik sırları değildir; devletler sıklıkla füze fırlatma kodları ya da deniz aşırı hava üslerinin yeri ile hiçbir ilgisi olmayan temel yönetim verilerini halktan saklamaktadır. Çoğu kez demokrasiler ve otoriter devletler benzer şekilde yanlış idare, yolsuzluk ya da kötü önceliklendirmeyi gizlemek için yönetim, finans ve sosyal verilere 'milli güvenlik sırları' muamelesi yapmaktadır. Bu gizlilik bazen açık bir milli güvenlik tehdidi olmasa da muhalefet gruplarını, siyasi partileri ya da vatandaşları gözetlemek için devlete ait gizlilik ve gözetleme aygıtlarının kullanılması şeklini almaktadır. Halkın bu şekilde aldatılması, iktidar partisi ya da liderinin halkı yanlış yönlendirerek ya da siyasi muhalefeti bastırarak yeniden seçilmeyi garantilemek için savaş zamanlarındaki milli güvenlik aygıtını kullandığı çatışma ve savaş zamanlarında dikkate değer ölçüde artmaktadır. Ülke dışındaki iç savaşlara müdahil olan Batı ülkeleri de asker zayiatı rakamlarını halktan ve medyadan gizleme eğilimi göstermektedir.

Tipik üst düzey demokrasiler olan Kanada ve Norveç örnekleri, gizliliğin nasıl tüm rejim türlerine bela olduğunu ortaya koymaktadır. 1970'lerde Kanada Güvenlik İstihbarat İnceleme Komitesi (Security Intelligence Review Committee - SIRC), 'sol eğilimli basın ve siyasi partilere yönelik haneye tecavüz, kundakçılık ve hırsızlık' eylemlerinden oluşan geniş kapsamlı gözetleme suistimalleri yaşandığını rapor etmiştir; ayrıca Kanada istihbaratının söz konusu programın kapsamı konusunda bir bakanlık soruşturma komisyo-

[11] Michael P. Colaresi, Democracy Declassified: The Secrecy Dilemma in National Security by Michael P. Colaresi (Oxford University Press, 2014).

nuna yalan söylediği 'müteakip bir örtbas etme' olayı da söz konusudur.[12] Kanada Atlı Polisinin icra mekanizması yoluyla, milli güvenlik kisvesi altında yerel muhalefet gruplarına ve partilerine sistematik olarak saldırılar düzenlenmiş ve dağıtılmıştır. Norveç'teki suistimaller 1970'lerde yaşanmış ve ancak 1990'larda Lund Komisyonu Raporunda ifşa edilebilmiştir.[13] Bu suistimaller Norveç polisi, istihbaratı ve Milli Güvenlik Kurumunun gizli ya da açık bir milli güvenlik tehdidi oluşturmayan ya da çok küçük bir tehdit oluşturan muhalefet gruplarının gözetlenmesi ve dağıtılması için yürüttüğü ortak çabaları kapsamaktadır.

İstihbaratı ve gizli bilgileri ele alan liderlerin ve karar verici grupların ikilemi, kamuoyunun rızasından kaynaklanmaktadır. Herhangi bir politikanın başarılı olabilmesi için kamuoyunun rızasının ve bunların uygulanması için sonuç olarak ortaya çıkacak mobilizasyonun mevcut olması gereklidir. Benzer şekilde, demokratik karar verme sistemleri yanlış hesaplama ya da yanlış algılama olasılıklarını ortadan kaldırmakta ve potansiyel olarak maliyetli hataların erken keşfedilmesine olanak vermektedir. Otoriter baskı, liderin hem aşırı vergilendirme ve yolsuzluk şeklinde halkın elindeki kaynakları zorla almasına hem de halkın rızası olmadan politikalar uygulamasına olanak verir. Bunun olumsuz tarafı, daha liberal sistemlerin üretim kapasitesi ve hızı nedeniyle, cebri yöntemler yoluyla üretilen kaynakların demokrasiler tarafından üretilen kaynaklara kıyasla genellikle daha kalitesiz olmasıdır. Teknik olarak demokratik liderler gerçekleri çarpıtarak ya da belirli türdeki bilgileri saklayarak yerel kamuoyunu yanlış yönlendirebilirler; ancak bu tür taktikler ifşa olduğunda, sürece dahil olanlar yasal işlemler de dahil olmak üzere orantısız bedeller ödeyebilirler.

Dijital Gözetleme - Türler ve Araçlar

Dijital gözetleme ve atlatma araçları dijital teknolojilerdeki ilerlemelere paralel olarak artmakta ve değişmektedir; teknoloji ne kadar hızlı ilerlerse, hem gözetleme yapmak hem de gözetlemeye karşı atlatma araçları kullanmak o kadar kolay hale gelmektedir. Bu açıdan, teknolojinin kendisi tarafsızdır ve kıyaslanabilir bir ölçüde yelpazenin tüm taraflarını desteklemektedir; ancak en yüksek malzeme, teknik, insan kalitesi ve insan gücü kabiliyetlerinin tümüne sahip olan taraf kaçınılmaz olarak teknolojik ilerlemelerin sonuçları üzerinde kontrole sahiptir. Dijital gözetleme kabaca veri güvenliği, görüntüler, ICT'ler, coğrafi konum ve biyometri alanlarına ayrılabilir. Bu araçların büyük kısmı geleneksel sinyal istihbaratı uygulamalarından geldiğinden, bunların temel amacı dış ve iç iletişimi, veri transferlerini ve ağları izlemektir.

Yığınsal Veri İzleme. Veri izleme, dijital iletişimin temel taşı olarak bilgisayar ve ağ gözetlemenin kesişim noktasında yer almaktadır ve hem sabit disk sürücüler ve USB bellek sürücüleri gibi fiziksel veri saklama birimleri, hem de İnternet tabanlı veri transferi, yerelleştirme ve bulut depolama uygulamaları ile ilgilidir. Bu tür gözetlemeden genellikle daha genel nitelikli dijital gözetleme terimi kapsamında bahsedilmektedir. Yığınsal veri izleme, tüm dijital olarak bağlı iletişim ve işlemlerin temel taşı olan 'paketler' yoluyla gerçekleşir. Paketler, içeriği ve tarih/saat, gönderici/alıcı ve transferin yeri ile ilgili bilgilerden oluşan meta veriyi içerir. Mesafe ne kadar olursa olsun, paketler üçüncü şahıs kurumlar ya da kuruluşlar tarafından izlenmelerine, derlenmelerine ve saklanmalarına olanak veren birkaç İnternet Santral Noktasından (IXP'ler) geçer. Örneğin deniz altındaki fiber-optik kablolara bağlantı yapılması iyi bilinen bir durumdur; bununla birlikte yığınsal veri izlemenin çoğu devletin İnternet Servis Sağlayıcılara (ISS'ler) yaptığı baskılar yoluyla gerçekleştirilir.

ICT İzleme. İnternet İletişim Teknolojisi (ICT) gözetlemesi hem Twitter, Facebook ya da Instagram gibi sosyal medya platformlarındaki insan faaliyetlerine, hem de Whatsapp, Telegram, Signal ya da basit SMS araçları gibi eşler arası iletişim araçlarına odaklanmaktadır. ICT gözetlemesi hem içerik (yani ilgili mesajın metni) ve meta veri (mesajın tarihi, saati, yeri) hem de tek bir bireyin ya da bir grubun ağı (takip/arkadaşlar, tekrar tweet, 'beğenme' örüntüleri) ile ilgilidir. ICT'leri gözetleyenler sadece devletler ya da istihbarat kurumları değildir; işverenler, okullar ve (örneğin kütüphaneler, restoranlar, okullar gibi) kamuya açık wi-fi sağlayıcıları da ICT izleme gerçekleştirmektedir. ICT'leri izleyen, tanımlayan ve kaydeden mobil iletişim izleme ekipmanları (IMSI Yakalayıcılar), müdahaleci yazılım (kötü amaçlı yazılımlar), ağ gözetleme, veri saklama sistemleri ve derin paket inceleme (DPI) yöntemleri, ICT içerik izlemenin en popüler türlerinden bazılarıdır.

[12] Justin Ling, "The Story of How Canadian Police Committed Arson to Stop a Black Panther Meeting," VICE News, Haziran 2017, https://news.vice.com/en_ca/article/eva8da/story-of-how-canadian-police-committed-arson-to-stop-a-black-panther-meeting.

[13] Dr Hans Born ve Ms Marina Caparini, Democratic Control of Intelligence Services: Containing Rogue Elephants (Ashgate Publishing, Ltd., 2013), 145.

Coğrafi Konum ve Uzaktan Algılama. Diğer gözetleme türlerinin içine de gömülü olmakla birlikte, konum gözetlemenin kendi belirgin özellikleri vardır. Mobil cihaz sinyallerine ve küresel konumlandırma sistemi (GPS) verilerine dayanan bu gözetleme türü, bir bireyin, grubun ya da bir binanın/tesisin izlediği yolu, uğradığı noktaları ve koordinatlarını çıkarmak için kullanılabilir. Londra, Brüksel, Paris ve New York dahil olmak üzere dünyadaki metropol kentlerin çoğunda polis faaliyetlerine, gözetlemeye ve davranış modellemesine yardımcı olan geniş bir CCTV kamera ağı bulunmaktadır. Bununla birlikte, konum gözetleme CCTV'lerin ortaya çıkışı ile önemli ölçüde evrilmiştir. LIDAR (Işık Tespiti ve Mesafe Tayini - lazer tabanlı bir havadan görüntü alma aracı), uydu ya da yüksek irtifa uçağı görüntü verileri ve coğrafi bilgi sistemi (GIS- coğrafi verileri tespit etmek, çıkarmak ve depolamak için tasarlanmış araçlara ait şemsiye isim) bu kategoriye girmektedir.

Biyometri. Her bir bireye özgü olduklarından, biyometrik işaretler en eşsiz kişisel bilgi türleridir. Örneğin parmak izi muhtemelen en eski ve en yaygın kullanılan biyometrik veri türüdür. Bununla birlikte teknolojik gelişmeler, gözetleme şirketlerinin daha yeni biyometrik veri türlerini toplamalarına ve izlemelerine olanak vermiştir. Yeni biyometrik tanımlayıcıların bazıları yüz/retina tanıma, ses tanıma, cilt yansıması ve termogramlardır. Alışveriş merkezleri, stadyumlar,bankalar, havaalanları ve ulaşım hizmetleri gibi yüksek insan akışının olduğu alanlarda çeşitli biyometrik gözetleme türleri gittikçe daha yaygın hale gelmektedir. Biyometrik verilerin öge boyutu ve uzun süreler boyunca kolayca saklanabilmeleri ve kullanılabilmeleri, özellikle yüksek nüfus yoğunluğuna sahip bölgelerde bunların popülerliğinin artmasına yol açmıştır. Örneğin Çin, 'Physicals for All' adlı bir program yoluyla tüm Sincan sakinlerinin biyometrik verilerini toplamaya başlamıştır; yaklaşık 11 milyon Sincan sakininin iris taramalarını ve kan gruplarını içeren bir veri tabanı oluşturulacaktır.

Nesnelerin İnterneti. IoT'ler (Nesnelerin İnterneti), makineler arasındaki otomatik iletişim üzerinde yapılandırılmış tüketiciye dönük cihazlardan oluşur. Günümüzde bulaşık makineleri, TV'ler, ev yardımcıları ve buzdolapları gibi evde kullanılan cihazların yaygın eşyaların çoğu IoT özelliğine sahiptir. Kullanıcılar, özel uygulamaları kullanarak uzaktaki bir konumdan perdelerini açıp kapatabilir, su sıcaklığını, yemek pişirmeyi ve ev ısıtma kontrollerini ayarlayabilir. Çoğu modern ev güvenlik ve alarm sistemleri de IoT özelliğine sahiptir, evlerin içine kurulmuş CCTV kamera grupları bulunmaktadır. Kullanıcılar, İnternet uygulamaları yoluyla bu kamera görüntülerini ve evlerini izleyebilmektedir. IoT'lerde toplanan ve saklanan veriler, örneğin eve ya da iş yerine varış zamanı ve buralarda geçirilen süre, konuşma-hareket tespiti, bireylerin ya da kurumların satın alma ve tüketim örüntüleri ile ilgilidir. Koruma tedbirleri olmazsa, IoT gözetlemesi evde ve iş yerlerinde geçirilen süre, yapılan çevrim-içi alışveriş türleri ve sosyal ağ (aile ve yakın arkadaş bilgileri) hakkında büyük ölçekli özel vatandaş bilgileri sağlayabilir, bu da vatandaşların günlük yaşamlarına kitlesel devlet müdahalesine olanak verir. Ancak söz konusu tehdit devletlerin de ötesine geçmektedir; çünkü bilgisayar korsanları da bireyleri gözetlemek ya da eşyalarının hatalı çalışmasına ve ciddi bedensel zarara yol açmak için IoT özellikli evlerden yararlanabilirler.

Geçen on yıllarda gözetleme endüstrisindeki büyümenin önemli bir yan ürünü, 'Gözetleme-Sınai Kompleksi' kavramının ortaya çıkmasıdır.[14] 'Gözetleme-Sınai Kompleksi' (SIC), iyi bilinen bir 2nci Dünya Savaşı sonrası kavramı olan ve bir ulusun silahlı kuvvetleri ile özel silah üretim şirketleri arasındaki simbiyotik bir ilişkiye delalet eden askeri-sınai kompleks (MIC) kavramından türemiştir. Bu ilişkiyi savunan argüman, ulusun silahlı güçlerinin acil ve sürekli değişen ihtiyaçlarına karşılık veren daha fazla askeri üretim ve geniş bir silah endüstrisinin idame ettirilmesi şeklindedir. Ancak en iyi bilinen argüman, A.B.D. Başkanı Dwight D. Eisenhower tarafından ifade edilmiştir; Eisenhower, silah endüstrisi şirketlerinin yabancı politika ve savunma politikası üzerinde orantısız bir etkisi olacağını ve en üst düzeyde askeri üretime sürekli bağlılık ve ulusal milli güvenlik tehdidi üzerinde yoğun bir etki için gerekli koşulları oluşturacağını ileri sürmüştür.[15] Askeriyenin büyük silah endüstrisi şirketlerine bel bağlamasının, bu şirketlerin Kongre üzerindeki etkisinin ve Kongre'nin askeri politika üzerindeki etkisinin kombinasyonu, A.B.D. politikasındaki çok sayıdaki 'bürokrasi-siyaset-işadamı üçgenlerinden' birini oluşturmuştur. Bu tür 'bürokrasi-siyaset-işadamı üçgenleri', A.B.D.'nin daha fazla çatışmaya dahil olmasını savunan lobi çalışmalarına büyük miktarlarda paraların akıtılması yoluyla sistemin demokratik işleyişini bozacak ve ülkeyi savaşa daha meyilli bir hale getirecektir.

[14] Kirstie Ball ve Laureen Snider, The Surveillance-Industrial Complex: A Political Economy of Surveillance (New York: Routledge, 2013); David Lyon, Kirstie Ball ve Kevin D. Haggerty, Routledge Handbook of Surveillance Studies (New York: Routledge, 2012).

[15] Eisenhower, Dwight D., "Farewell address." Washington, DC 17 (1961).

SIC benzer bir mantık izlemektedir; ancak teknoloji şirketleri ile devletler arasındaki ilişki, MIC'de olduğu gibi karşılıklı yarar sağlayan bir ilişki değildir. Ayrıca, A.B.D. politikası ile sınırlı da değildir. SIC daha çok ulusun güvenlik ve istihbarat kurumlarının özel sektör teknoloji ve gözetleme şirketleri ile tek taraflı çıkarıcı bir ilişkiye girmesi anlamına gelir. Devletler ve istihbarat kurumları, bir kamu-özel gözetleme rabıtası yaratarak, özel şirketler tarafından işlenen büyük miktarlarda vatandaş verisini - çoğu kez hukuk dışı şekilde - kontrol altına alırlar ve bu şirketlere istediklerini yaptırmak için uygulama gücünü elde tutarlar. Devlet kurumlarının özel sektör veri tabanlarına erişimi hem yasal hem de demokratik sorunlar yaratmaktadır, çünkü çoğu devlet söz konusu gözetleme uygulamalarının kapsamını sınırlayan kanunların yayınlanmasından önce büyük miktarlarda özel vatandaş verisini zaten toplamış durumdadır. Bu tür yasalar mevcut olsa dahi, gözetleme teknolojilerinin evrilme hızı mevcut yasaları hızla hükümsüz hale getirmekte ve kurumların daha yeni dijital gözetleme biçimlerini kullanmak amacıyla kanunların ve mevzuatın etrafından dolaşmasına olanak vermektedir.

Devletler SIC'den üç ana fayda elde etmektedir. Birincisi, büyük miktarlarda yapılandırılmamış kişisel verinin ayrıntılı profil oluşturmaya olanak veren merkezi bir bağlantı noktasına toplandığı bir 'küme istihbarat ağı' oluşturmaktadır. İkincisi, gözetlemenin siyasi ve finansal maliyetleri devletlerden teknoloji şirketlerine geçmektedir. Normalde, kitlesel dijital gözetleme yapabilmek için kurumların fiziksel altyapıya (süper bilgisayarlar) ve iyi eğitimli insan sermayesine (veri bilimciler, mühendisler) yatırım yapması gerekecektir. Devletler, SIC yoluyla, teknoloji şirketleri tarafından harcanan önemli miktardaki esas maliyetten bedava yararlanabilmektedir. Üçüncüsü, gözetleme programının açığa çıkması halinde seçmen maliyetlerinin büyük bir bölümü (eleştiriler ve toplum önünden küçük düşme) kurumların kullanıcıların emanet ettiği kişisel verileri toplamalarına ve kullanmalarına izin verdikleri için devletten ziyade şirketler tarafından karşılanacaktır. SIC, günümüzün teknoloji ortamında, benzeri görülmemiş miktarlarda ve öge boyutunda özel veri elde edilmesine olanak sağlayarak devletleri geniş kişisel bilgi ağlarının merkezleri haline getirmiştir. Ancak SIC öte yandan devletleri daha savunmaya dönük hale getirerek ve veri ve sistem yerelleştirmesi isteme konusunda daha zorlayıcı kılarak uzun vadede bir güvenlik ikilemi yaratmaktadır. Veri ve bilgilerin serbest akışı ticaret, finans ve küresel karşılıklı bağlantılılık için esas kabul edilmekle birlikte, dünyadaki istihbarat kurumlarının veri transferinin geçiş noktalarına (bulut sistemleri, deniz altındaki fiber optik kablolar) müdahalesi yerelleştirmeye yönelik taleplerin artmasına yol açmıştır. Ülkeler, sistemlerini ve verilerini yerelleştirerek, yabancı kurumların müdahale etmesini önlemek yoluyla 'veri milliyetçiliğini' vurgulamaya ya da yığınsal veri toplama durumunda milli verilerini güvenceye almaya çalışmaktadır. Ancak yerelleştirme söz konusu verileri siber saldırılara karşı gittikçe savunmasız bir hale getirmekte ve sıfırdan fiziksel depolama sistemlerinin kurulmasını, iyi eğitimli insan varlıklarının istihdam edilmesini ve depo koruma ağlarının oluşturulmasını gerektirerek veri koruma maliyetlerini arttırmaktadır. Veri yerelleştirmenin ticareti, transferleri ve finansı yavaşlatan uluslararası ölçekte istenmeyen bir hareket olmasına rağmen, temel vatandaş verilerinin yabancı istihbarat kurumlarına açık olması dikkate alındığında gittikçe daha fazla ülke yerelleştirmeyi gerekli bulmaktadır.

Dijital Gözetlemede Mevcut Eğilimler

Gözetleme-özel hayatın gizliliği savaşı, teknolojik gelişmelere adapta olmamızla ilgili daha büyük sorunlarımızın bir yan ürünüdür. Bu nedenle özel hayatın gizliliğine yönelik tehditler ile koruma çözümleri genellikle sıkı bir kronolojik sırayla birbirlerini izlemiştir. Örneğin 'yalnız kalma hakkı' ilk kez 1890'larda ortaya çıkmıştır. Aynı on yılda, insanların kimliklerini belirlemek ve kişisel kimliklerin iyi korunmuş fiziksel veri kümelerini oluşturmak için parmak izi kullanılmaya başlanmıştır. ABD'de 1928 yılındaki bir mahkeme kararında 'milli güvenliğe yönelik tehditler' söz konusu olduğunda elektronik iletişime el konulması lehinde bir hükme varılmıştır, ancak milli güvenliğin ne olduğu konusuna değinilmemiştir. MINARET ve SHAMROCK Projeleri, 1967-78 dönemini kapsayan ve FBI-CIA, BNDD (Narkotik ve Tehlikeli Uyuşturucular Bürosu) ve DoD'nin (Savunma Bakanlığı) SSCB'ye karşı yerel karşı-casusluk görevi görmesi amaçlanan koordineli çabalarıyla ABD vatandaşlarının tüm elektronik haberleşmelerinin izlendiği ve derlendiği iki ABD Hükümeti uygulamasıdır.[16] 1967 yılında, 'ABD'ye karşı Katz' davası emniyet kurumlarının kişisel iletişimleri izlemeden önce bir izin almasını hükme bağlayan bir içtihada vesile olmuştur.[17] Parmak izlerinin dijitalleştirilmesi

[16] Robert N. Davis, "Striking the Balance: National Security vs. Civil Liberties," Brooklyn Journal of International Law 29 (2004 2003): 175–238; Laura K. Donohue, The Future of Foreign Intelligence: Privacy and Surveillance in a Digital Age (Oxford: Oxford University Press, 2016).

[17] Amerika Birleşik Devletlerine karşı Katz, 389 U.S. 347 (1967): https://supreme.justia.com/cases/federal/us/389/347/case.html

ve vatandaş bilgilerini içeren büyük kişisel veri kümelerinin oluşturulması ile, dijital kimlik hırsızlığı yaygın hale gelerek müdahale önleyici ve virüs önleyici yazılım sektöründeki hızlı büyümeye yol açmıştır. 1995 yılında HTTPS'nin ortaya çıkışının ardından, casus yazılımlar ve yazılım hataları sıradan hale gelmiş ve 2000'lere girerken virüs önleyici ve kötü amaçlı yazılım önleyici şirketlerin siyasi açıdan gittikçe daha alakalı hale gelmesine neden olmuştur. Bu özellikle büyük ölçekli fiziksel bir tahribat olasılığına işaret eden bir bilgisayar virüsü olan Stuxnet'in ortaya çıkarılmasından ve yeni 'hava aralığı' biçimlerinin ve koruma mekanizmalarının keşfinden sonra söz konusu olmuştur.[18] Snowden ifşaatlarının ve NSA gözetleme canavarının kapsamının ortaya çıkarılmasının ardından, kamu-düzeyinde kitle kaynaklı özel hayatın gizliliği ve anonimlik ağlarının çoğalmasının yanı sıra AB 'Unutulma Hakkı' kavramını ortaya koymuştur.[19]

Gözetlemenin tarihçesi oldukça eski olmakla birlikte, modern dijital ve karşılıklı olarak bağlantılı gözetleme tartışmalarının anlamlı bir izi 11 Eylül sonrası güvenlik ortamına kadar sürülebilir. Dijital gözetlemeye (yığınsal meta veri toplama, biyomedikal gözetleme ve ağ izleme gibi) ilişkin modern tartışmalarımızın büyük kısmının doğduğu nokta daha çok 11 Eylül sonrası ABD gözetleme uygulamalarıdır. Bu George W. Bush dönemi programların ve bunlara meşruluk kazandırmaya yönelik yasal-yasama adımlarının çoğu Avrupa ülkelerini etkilemiş ve dünyanın geri kalanı için önemli örnekler ve devlet davranışı standartları teşkil etmiştir. Amerika Birleşik Devletleri'nde Ulusal Güvenlik Kurumu (National Security Agency - NSA), 2001 tarihli Vatanseverlik Yasasından sonra gözetleme tedbirlerinin yasal olarak kolaylaştırılmasını takiben ABD vatandaşlarının telefon görüşmelerini, e-postalarını ve diğer dijital faaliyetlerini bir izin gerekmeden toplamaya ve saklamaya başlamıştır. ('Stellarwind'[20] adlı bir Bush dönemi programı altındaki) bu tür uygulamalar büyük ölçüde kamunun bilgisi olmadan yürütülmüş ve program ancak 2008 yılında Kongre'nin dikkatini çekmişti. Kongre söz konusu programı 2008 yılında harici devlet aktörler ve casusluk ve terör şüphelisi bireyler ile ilgili fiziksel ve elektronik gözetleme verilerinin işlenmesine yönelik ABD yasal prosedürlerini belirleyen Yabancı İstihbarat Gözetim Yasasının (Foreign Intelligence Surveillance Act - FISA) yetki alanına sokmuştu. O günden bu yana, söz konusu yasada yer alan ihtilaflı Kısım 702 ("yabancı terörist tehditleri dahil olmak üzere, hükümetin Amerika Birleşik Devletleri dışında bulunan yabancıların iletişimlerini elde etmesine izin verir"[21]) gittikçe artan bir ihtilaf ve siyasi tartışma konusu olmuştur. Yasa, geniş bir şekilde tanımlanmış 'yabancı istihbarat operasyonları' amaçlarına yönelik olarak, telekomünikasyon şirketlerine mevcut erişimi genişletmeye ek olarak ABD kurumlarının Silikon Vadisi şirketlerine erişimini yasal hale getirmiştir.[22] Kongre'nin yasanın aşırılığı konusunda yaygın şekilde eleştirilmesine ve medyada konuyla ilgili farkındalık oluşturma çabalarına rağmen Kongre yasayı 2012'de 5 yıllığına uzatmıştır.

Gözetleme-özel hayatın gizliliği tartışmasında belki de en önemli dönüm noktası, ABD casusluk programlarının kapsamına, derinliğine ve hukuk dışı boyutuna ilişkin ayrıntıları veren 2013 NSA 'Snowden' sızıntılarıdır.[23] Booz Allen Hamilton için çalışan bir NSA yüklenicisi olan Edward Snowden yaklaşık 1,5 milyon milli istihbarat dosyasını indirmiş, bunları basına sızdırmış ve önce Hawaii'deki üssünden Hong Kong'a kaçmış ve daha sonra Moskova'da kısılıp kalmıştı. 'Snowden sızıntıları', NSA tarafından toplanmış milyonlarca Verizon telefon kaydını içermekteydi; bu, siber saldırılar için deniz aşırı hedeflerin toplanmasına yönelik Obama dönemindeki bir emre ve ABD vatandaşlarının İnternet ve e-posta meta verilerini gerçek zamanlı olarak kaydeden 'EvilOlive' adlı bir NSA programına dayanmaktaydı.[24] Sızıntılar ayrıca İngiliz Devlet İletişim Merkezi (Government Communications Headquarters) GCHQ'nun 2009 yılında Londra'da yapılan G-20 toplantılarına katılan siyasetçileri nasıl dinlediğini ve e-posta mesajlarını, Facebook paylaşımlarını, tarayıcı geçmişlerini ve İnternet aramalarını izlemek ve kataloglamak için fiber-optik kablolara

18 R. Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon," IEEE Security Privacy 9, no. 3 (Mayıs 2011): 49–51, https://doi.org/10.1109/MSP.2011.67.

19 Jeffrey Rosen, "The Right to Be Forgotten Symposium Issue: The Privacy Paradox: Privacy and Its Conflicting Values," Stanford Law Review Online 64 (2012 2011): 88–92.

20 David L. Altheide, "The Triumph of Fear: Connecting the Dots about Whistleblowers and Surveillance," International Journal of Cyber Warfare and Terrorism (IJCWT) 4, no. 1 (1 Ocak 2014): 1–7, https://doi.org/10.4018/ijcwt.2014010101.

21 FISA Kısım 702: https://intelligence.house.gov/fisa-702/

22 Stephanie Cooper Blum, "What Really Is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform," Boston University Public Interest Law Journal 18 (2009 2008): 269–314.

23 S. Landau, "Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations," IEEE Security Privacy 11, no. 4 (Temmuz 2013): 54–63, https://doi.org/10.1109/MSP.2013.90.

24 Glenn Greenwald ve Spencer Ackerman, "How the NSA Is Still Harvesting Your Online Data," the Guardian, 27 Haziran 2013, http://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection.

düzenli olarak kaçak bağlantı yapma uygulamasını ve bu bilgileri NSA ile paylaştığını ortaya çıkarmıştı.[25] Devlet sırlarını ortaya sermesi Snowden'i ABD'de bir halk düşmanı haline getirmiş olmakla birlikte, dünyanın geri kalanında bu ifşaatlar üst düzey normlar oluşturulması ve yasal düzenlemeler için önemli bir küresel ivme başlatmıştır. Hatta bu süreç, kitlesel gözetleme düzenlemelerinin ne kadar aşırı hale geldiğine tanık olan STK'leri, uluslararası şirketleri ve bireysel vatandaşları da telaşa düşürmüştür. Bu durum vatandaşların öncülük ettiği özel hayatın gizliliği inisiyatifleri konusunda yeni bir dönem başlatmış, yeni atlatma araçlarının ortaya çıkmasına ve yasama organları üzerinde casusluk faaliyetlerini demokratikleştirmeye ve meşrulaştırmaya yönelik önemli baskılara yol açmıştır. Ayrıca, hem devletler arası rekabet hem de yabancı dijital istihbarat faaliyetlerinin yerel olarak izlenmesi için kendi gözetleme kabiliyetlerini güçlendirmeye yönelik önlemler alan uluslar, hatta NATO müttefikleri arasında yeni bir karşılıklı güvensizlik statükosuna ve istihbarat güvenliği ikilemine neden olmuştur.

Şu anda ABD, Rusya ve Çin, teknoloji şirketlerini istihbarat kurumlarının istediklerinde cihazlardaki bilgilere erişebilmeleri için şifrelemenin ve kullanıcı parolalarının üstesinden gelmelerine olanak verecek 'arka kapılar'[26] oluşturmaya zorlamaktadır. ABD teknoloji şirketleri ayrıca kaynak kodlarını inceleme için açmaları konusunda Çin'in baskısı altındadır. Çin'in bakış açısına göre, bu kaynak kod denetimi söz konusu cihazlara entegre edilmiş olası ABD 'casus yazılımlarını' atlatmak için gereklidir.[27] Öte yandan Washington'ın savı, ABD'nin Çin'e giden teknoloji ihracatına arka kapılar koymakla ilgilenmediği, ancak daha çok söz konusu denetim süreçlerinin teknoloji şirketlerine ABD yapımı cihazlara Çin casus yazılımları kurmaları yolunda baskı yapabileceğinden endişelendiği yönündedir.[28] Teknoloji ihraç eden ülkelerin çoğunun teknoloji ihracatı ve ithalatında kendi arka kapı versiyonlarını ya da kaynak kod denetim süreçlerini oluşturmalarının nedeni bu casus yazılım ikilemidir. Benzer şekilde hem NSA hem de GCHQ küresel internet iletişimini izlemek ve toplamak için deniz altındaki fiber-optik kablolara kaçak bağlantı yapmak için denizaltıları kullanmışlardır.[29]

ABD gözetleme uygulamaları ile otoriter rejimlerin gözetleme uygulamaları arasında net bir çizgi çekmek zordur, aradaki tek fark düzenlemelerin yönüdür. Çoğu demokraside, gözetleme uygulamalarının sızması ve devlet dışı taraflarca keşfedilmesi yasal denetim gereksinimini tetiklerken, mevzuatın yönünü denetim ihtiyaçlarının değil milli güvenlik gereksinimlerinin belirlediği otoriter ülkelerde denetimin boyutunu istihbarat gereksinimleri belirlemektedir. Örneğin Rusya'da, Sistem Operasyon-Araştırma ile İlgili Önlemler (SORM) uzun süredir dijital iletişimin ve telekomünikasyon ağlarının yasalara uygun şekilde gözetlenmesi için temel oluşturmaktadır.[30] Gözetlemenin yasal sınırlarını belirleyen bir hukuki ve teknik gereklilikler kümesi olan SORM bugüne dek üç kez güncellenmiştir; SORM-1 (tüm telekom operatörlerine Federal Güvenlik Servisi FSB'nin donanımlarının zorunlu olarak kurulması) 1995'te, SORM-2 (İnternet Servis Sağlayıcıların sunucularına ilave FSB donanımlarının kurulması) 1998'de ve SORM-3 (IPv4-IPv6 ağları, IMSI-IMEI verileri ve POP, SMTP ve IMAP4 adresleri için ayrı şartlar içeren, hedeflenmiş dijital gözetlemeye yönelik daha ayrıntılı bir dinleme sistemi) ise 2014'te uygulamaya konmuştur. SORM hukuki açıdan gözetleme kurumlarına bir izin gerekmeksizin meta verileri izleme ve kaydetme olanağı vermektedir, ancak içerik için hala bir izin gereklidir. Kurumların bir izin mevcut olduğunda dahi izni hedef ISS'ye ya da şirkete gösterme zorunlulukları yoktur; izin sadece kurum içi denetim amaçlarına yöneliktir. 2016 yılında (adını iktidardaki Birleşik Rusya Partisinin kıdemli bir üyesi olan Irina Yarovaya'dan alan) 'Yarovaya Kanunu' bu kısıtlamaları daha da kolaylaştırmış ve tüm ISS'lerin ve iletişim şirketlerinin kurumun isteği üzerine tüm meta verileri bir izin gerekmeksizin otomatik olarak aktarmaları hükmünü getirmiştir.[31]

---

[25] Source: BBC/Panorama, "Edward Snowden: GCHQ Wants to Own Your Phone – Video," The Guardian, 5 Ekim 2015, sec. US news, http://www.theguardian.com/us-news/video/2015/oct/05/edward-snowden-gchq-wants-own-your-phone-video.

[26] "Hacker Lexicon: What Is a Backdoor?," WIRED, 28 Mart 2018'de erişilmiştir, https://www.wired.com/2014/12/hacker-lexicon-backdoor/.

[27] Dave Lee, "China and US Clash over Backdoors," BBC News, 4 Mart 2015, sec. Technology, http://www.bbc.com/news/technology-31729305.

[28] Ben Goad, "New Pressure on US Tech to Comply with China's Access Demands," Text, TheHill, 16 Ekim 2015, http://thehill.com/policy/cybersecurity/257194-new-pressure-on-us-tech-to-comply-with-chinas-access-demands.

[29] Ewen MacAskill ve ark., "GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications," the Guardian, 21 Haziran 2013, http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

[30] Andrei Soldatov ve Irina Borogan, "Inside the Red Web: Russia's Back Door onto the Internet – Extract," the Guardian, 8 Eylül 2015, http://www.theguardian.com/world/2015/sep/08/red-web-book-russia-internet.

[31] Alec Luhn, "Russia Passes 'Big Brother' Anti-Terror Laws," the Guardian, 26 Haziran 2016, http://www.theguardian.com/world/2016/jun/26/russia-passes-big-brother-anti-terror-laws.

Öte yandan, Çin gözetleme sistemine büyük ölçüde Tibet ve Sincan-Uygur ihtilafları yön vermektedir.[32] Çin'in gözetleme kanunu, yasal gerekliliklerin yönü (yani güvenlik ihtiyaçlarının yönlendirdiği yasalar) açısından Rusya'nınkine benzerdir; ancak Çin bir adım daha ileri gitmekte ve vatandaşların ihlalleri ve şüpheli dijital faaliyetleri izleme konusunda devlet kurumlarına yardımcı olmalarını gerektiren 'sosyal denetlemeyi' teşvik etmektedir.[33] Yakın zamandaki yasal gerekliliklerin bazıları arasında çevrim-içi video yüklemeleri için gerçek ismin zorunlu olarak kaydedilmesi, Çin vatandaşlarının ulusal gözetlemede yer almalarına olanak veren devlet yapımı raporlama ve şikayet uygulamaları, vatandaşların sosyal davranışlarını 'derecelendiren' sosyal kredi sistemi, yığınsal biyomedikal veri toplama ve kataloglama, gerçek zamanlı yüz tanıma veri tabanı ve ülkenin 20 milyondan fazla CCTV kamerasının Yapay Zeka tabanlı izlenmesi yer almaktadır.[34] Çin, 28 Haziran 2017 itibariyle, Milli Güvenlik Bakanlığına ve Kamu Güvenliği Bakanlığının İç Güvenlik Bürosuna herhangi bir izin gerekmeksizin istediklerinde tüm dijital vatandaş ve şirket verilerini toplamalarına yönelik kapsamlı yasal yetki veren yeni bir Milli İstihbarat Kanununu kabul etmiştir.[35] Kanun, yasal bir denetim mekanizması oluşturmaktan özellikle kaçınmaktadır; ancak söz konusu istihbarat faaliyetlerini 'liderlik çekirdeğinin', yani Komünist Parti Başkanı Xi Jinping'in siyasi izlemesine tabi kılan siyasi bir denetleme mekanizması mevcuttur.

ABD, Çin ve Rusya'ya kıyasla Avrupa Birliği ülkeleri biraz farklı bir yol izlemektedir. AB vatandaşlarının kişisel bilgilerinin ve kamusal verilerin Amerika Birleşik Devletlerine hukuki transferine olanak sağlayan bir veri paylaşım anlaşması olan 2000 'Güvenli Liman' anlaşmasının (2000/520/EC) imzalanmasından 15 yıl sonra, Avrupa Birliği Adalet Divanı (CJEU) 2015 yılında Snowden-dönemi hukuk dışı kitlesel gözetleme ifşaatlarının söz konusu verilerin ABD'li ortaklar ile paylaşıldığında yeterince korunabileceğini tespit etmeyi imkansız kıldığı yolunda bir karar vermiştir.[36] Bu durum ABD ile AB arasında önemli bir bölünmeye yol açmıştır; AB, ABD'nin Avrupa kişisel veri mimarisine girmeye yönelik yasa dışı gözetleme talimatlarını önlemeye çalışmıştır. Bununla birlikte, gizlilik-özel hayat ikilemi bireysel Avrupa ülkelerinde de sona ermektedir. İngiltere Kasım 2017'de GCHQ'ya 'deniz aşırı ile ilgili' dijital faaliyetleri kitlesel toplama, kataloglama ve izleme izni veren Soruşturma Yetkileri Yasasını (IPA) kabul etmiştir.[37] Bu Yasa, dünya genelindeki dijital ağlara kitlesel korsan girişin yanı sıra büyük miktarlarda iletim, meta veri ve ekipman (donanım verileri) toplama yetkisi veren bir izin yoluyla 'yığınsal veri edinimi' için yasal bir zemin sağlamaktadır. Yığınsal toplamanın ardından üç tane siyasi ve hukuki denetim mekanizması katmanı mevcuttur. İstihbarat servisinin başının ya da bir temsilcisinin Dışişleri Bakanına resmi bir gerekçe sunması gereklidir. Ardından İçişleri Bakanlığının, hukuki uygunluk için Adli Yargıca gönderilen bir rapor olan dahili bir orantılılık analizi yapması gereklidir. 'Çifte kilit mekanizması' (suistimale karşı hem hukuki hem de siyasi koruma tedbirleri) adı verilen bu tedbir 6 ay süreyle yığınsal toplamaya olanak vermektedir ve aynı süreç yoluyla yenilemeye tabidir.[38] Yasadaki mevcut bir sorun, söz konusu kurumların bir suistimali ya da hatalı kararı durumunda yabancı bir bireyin ne gibi önlemlere başvurabileceğini belirlememiş olmasıdır.

Öte yandan Almanya'da Ekim 2017'de çıkarılan 'İletişim İstihbarat Toplama Yasası', Federal İstihbarat Servisine (BND) Almanya'da bulunan çok sayıdaki noktanın yanı sıra deniz aşırı İnternet Santral Noktalarından (IXP) yığınsal toplama yetkisi vermiştir; Almanya'da bulunan noktalar bu ülkeyi dünya genelindeki diğer istihbarat kurumlarının gözetleme faaliyetlerinin yanı sıra dünya genelindeki İnternet trafiğinde eşsiz bir oyuncu haline getirmektedir.[39] Yasanın görünüşteki 'yerel' ilgisine rağmen, Almanya'daki IXP'lerin fiziki konumu yasayı gerçekte küresel ve BND'yi

[32] Tom Phillips, "China Testing Facial-Recognition Surveillance System in Xinjiang – Report," the Guardian, 18 Ocak 2018, http://www.theguardian.com/world/2018/jan/18/china-testing-facial-recognition-surveillance-system-in-xinjiang-report.

[33] Anna Mitchell ve Larry Diamond, "China's Surveillance State Should Scare Everyone," The Atlantic, 2 Şubat 2018, https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/.

[34] Rachel Botsman, "Big Data Meets Big Brother as China Moves to Rate Its Citizens," WIRED UK, Ekim 2017, http://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion.

[35] "China Passes Tough New Intelligence Law," Reuters, 28 Haziran 2017, https://www.reuters.com/article/us-china-security-lawmaking/china-passes-tough-new-intelligence-law-idUSKBN19I1FW.

[36] Samuel Gibbs, "What Is 'Safe Harbour' and Why Did the EUCJ Just Declare It Invalid?," the Guardian, 6 Ekim 2015, http://www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection.

[37] Scott Carey, "Investigatory Powers Act: What You Need to Know," ComputerworldUK, Ocak 2018, https://www.computerworlduk.com/security/draft-investigatory-powers-bill-what-you-need-know-3629116/.

[38] Privacy International, "A New Era of Mass Surveillance Is Emerging Across Europe," Medium (blog), 17 Ocak 2017, https://medium.com/privacy-international/a-new-era-of-mass-surveillance-is-emerging-across-europe-3d56ea35c48d.

[39] Jenny Gesley, "Foreign Intelligence Gathering Laws: Germany," Web sayfası, Haziran 2016, https://www.loc.gov/law/help/intelligence-activities/germany.php.

sistemik gözetleme tartışmasında önde gelen bir oyuncu haline getirmektedir.[40] Bu yasada BND'ye, bir milli güvenlik sorunu oluşturabilecek terimleri ve sözcük alışverişlerini yakalamak için büyük veri ve veri-olarak-metin yapay zeka öğrenimi uygulamalarını kullanan bir 'ilgililik testi' yapmaya yönelik bir ön yetki verilmektedir. Bu testler BND tarafından herhangi hukuki ya da siyasi denetim olmadan yapılmaktadır, tek yetkili Kurumun Yöneticisidir. Söz konusu sözcüklerin, toplama amacına bağlı olarak iki ila dört hafta sonra silinmesi gerekmektedir. Alman Anayasa Mahkemesi, kamu menfaatine kıyasla 'listenin son derece yüksek önemi' nedeniyle BND'nin bu arama ve gözetleme terimlerini Alman Parlamentosunun Snowden sızıntılarının hemen ardından kurulan Bilgi Toplama Komisyonuna ifşa etmemesi yolunda daha önceden, Haziran 2013'te bir karar vermiştir.[41] İngiltere'ye benzer şekilde, BND'nin başının gerekli yığınsal toplamanın süresine ve kapsamına ilişkin ayrıntıları içeren resmi bir raporla Federal İdareye resmi olarak başvurması gereklidir; azami istek süresi 9 aydır. İki bağımsız yargıç ve bir federal savcıdan oluşan 3 üyeli bir değerlendirme komitesinin hukuki açıdan bir karar vermesi gereklidir. Bu heyet aynı zamanda 9 aylık sürenin yenilenmesi ve ayrıca suistimaller durumunda toplama sürecinin iptal edilmesi kararlarını veren esas makamdır.

Fransa, Kasım 2015'te Paris'te yaşanan saldırıların ardından, GCHQ ve BND'ye tanınan yetkilere benzer şekilde Dış Güvenlik Genel Müdürlüğüne (DGSE) yabancı ülkelere giden ve bu ülkelerden gelen dijital verilere kaçak bağlantı yapma, bunları kataloglama ve depolama olanağı veren Uluslararası Elektronik İletişim Yasasını kabul etmiştir.[42] İngiltere ve Almanya'nın aksine, Fransa'daki durumda yığınsal toplamayı doğrudan talep eden DSGE'nin başı değildir; Başbakanlığa bir istek gönderebilecek olan Savunma, İçişleri ya da Maliye Bakanına başvurması gerekmektedir. İstek yapıldıktan sonra, iletişim içeriği saklama süresi bir yıla kadar, iletişim meta verileri için ise 6 yıla kadardır.[43] İlave isteklerle şifreli içerik ve meta veriler 8 yıla kadar süreyle saklanabilir. Başbakanlığın kararından sonra - karardan önce değil, çünkü yasa yığınsal toplama kararı için bağımsız herhangi bir kuruma danışılmasını gerektirmemektedir - 9 üyeden (2 yargıç, 2 Danıştay üyesi, 4 milletvekili, bir elektronik iletişim uzmanı) oluşan Güvenlik İzlemelerinin Kontrolü Milli Komisyonuna (CNCIS) hukuki uygunluk için bilgi verilir. CNCIS ancak karardan sonra ve ancak bir bireyin ya da kurumun resmi şikayetinin ardından soruşturmalar ve incelemeler başlatabilir.

ABD, Rusya ve Çin'e kıyasla özel hayatın gizliliği, koruma tedbirleri ve yasal denetim konularında nispeten daha ilgili olmakla birlikte, Avrupa yasaları da suistimale karşı düzgün denetim mekanizmaları ve koruma tedbirleri açılarından açıkça muğlaktır. En sıkı durum olan İngiltere'de bile, Adli Yargıçların ne kadar inceleme yapabileceğine ilişkin sınırlar söz konusudur, ayrıca yığınsal veri toplama isteğinin ivediliği ile isteği onaylamak için gerekli yasal ve teknik denetimin süresi arasında önemli bir zaman baskısı mevcuttur. Üstelik, Avrupa'daki bu üç hukuki durumun tümü, toplanan yığınsan verilere ilişkin istihbarat paylaşımını ulusal yasaların kapsamı dışında bırakmaktadır. Eleştiriler, gözetleme suistimallerinin büyük bölümünün, iç ilişkiler dahilinde denetimi vurgulayan yerel koruma tedbirlerinden ziyade, dış ilişkiler ile ilgili olan istihbarat paylaşımı mekanizması içinde kolayca gerçekleşebileceğine işaret etmektedir.[44] Avrupa genelinde yükselişe geçen aşırı sağ ve seçimlerde gördüğü rağbet, kısıtlayıcı kitlesel gözetleme yetkilerini popüler hale getirmiştir. Gözetleme teknolojisi öncüleri olan ABD, Çin ve Rusya'nın oluşturduğu Orwellci örnekler ışığında, Avrupa ülkeleri de küresel gözetleme yarışında geride kalmama konusuna gittikçe daha fazla ilgi gösterir hale gelmektedir. Tipik bir güvenlik ikilemi senaryosunda, sinyal istihbaratı kurumlarına sıkı denetim ve hukuk bağları uygulayan ülkeler, dijital istihbaratın gittikçe artan üretilme ve işlenme hızına daha yavaş ve çoğu kez geç karşılık vermek zorunda kalmaktadır. Hem Avrupa İnsan Hakları Mahkemesinin hem de Avrupa Birliği Adalet Divanının mevzuatları, insan hakları endişeleri, istihbarat rekabeti ve gözetleme politikalarının seçimlerde gördüğü büyük rağbet arasında denge kurması gereken münferit Avrupa ülkelerinde gittikçe daha alakasız hale gelmektedir.

---

40 Andre Meister, "How the German Foreign Intelligence Agency BND tapped the Internet Exchange Point DE-CIX in Frankfurt, since 2009," netzpolitik.org (blog), 31 Mart 2015, https://netzpolitik.org/2015/how-the-german-foreign-intelligence-agency-bnd-tapped-the-internet-exchange-point-de-cix-in-frankfurt-since-2009/.

41 Marcus Lütticke, "New Leaks Show Germany's Collusion with NSA | DW | 21.06.2014," DW.COM, Haziran 2014, http://www.dw.com/en/new-leaks-show-germanys-collusion-with-nsa/a-17726141.

42 Kim Willsher, "France Approves 'Big Brother' Surveillance Powers despite UN Concern," the Guardian, 24 Temmuz 2015, http://www.theguardian.com/world/2015/jul/24/france-big-brother-surveillance-powers.

43 Nicolas Boring, "Foreign Intelligence Gathering Laws: France | Law Library of Congress," web sayfası, Aralık 2014, https://www.loc.gov/law/help/foreign-intelligence-gathering/france.php.

44 Cynthia Wong, "Big Brother Is Watching: Why We Should Fear Surveillance in the New World Order," Newsweek, 7 Şubat 2017, http://www.newsweek.com/state-surveillance-europe-populism-cctv-citizens-553857.

Kamu Tepkisi: Özel Hayatın Gizliliği ve Mahremiyet Araçları

Atlatma araçlarının sofistikeliği kısmen teknolojik ilerlemelerden, ancak büyük ölçüde devletler, teknoloji şirketleri ve vatandaşlar arasında gözetleme uygulamalarının boyutu ve derinliği konusunda güçlü bir hukuki ve siyasi akit bulunmamasından kaynaklanmaktadır. Bu demokratik ve hukuki boşluk, vatandaşları özel hayatın gizliliği konusunda kendi savunmalarını aramaya zorlamış ve gizliliğin ve anonimliğin karmaşık ve sürekli değişen örüntülerinin lehine önemli bir ivme yaratmıştır. Yani, istihbarat kurumlarının ulusal ve uluslararası yasalara uymamaları[45] ve bunun yanı sıra ulusal yasaların ya da denetimin yokluğu/zayıflığı, bireyleri ve aktivistleri bir 'kendi kendine yardım' refleksine itmiş ve güvenilir atlatma rejimleri ve kişisel kimlik ve veri koruma önlemlerine ilişkin farkındalık oluşturulmasına yönelik güçlü ve istikrarlı bir ivme ortaya çıkarmıştır. Bir atlatma aracını bir anonimleştirme aracından ayıran fark, atlatma aracının bir ağ ya da web sitesi kısıtlamasını baypas etmek için tasarlanmış olması, anonimleştirme aracının ise bir kullanıcının kimliğini korumayı amaçlamasıdır.[46] Bu araçlar sıklıkla birbirlerinin yerine kullanılmaktadır; örneğin randomize edilmiş yeniden yönlendirme tabanlı şifreli bir atlatma sistemi olan Tor, asıl amacı filtreleme ve engelleme uygulamalarını atlatmak olmasına rağmen, bilgileri anonim hale getirerek bir kullanıcının mahremiyetini korumak için kullanılabilir.[47]

Üç ana çevrim-içi kimlik türü mevcuttur: 'işlemsel kimlik', bir bireyin belirli bir görevle ilgilenmesine ya da bankalar, devlet ya da sigorta şirketleri gibi bir şirket ya da kuruluş ile işlemsel bir ilişkiye girmesine olanak veren dar-tanımlı bilgi kümesi anlamına gelir. 'Sosyal kimlik', metinler (örneğin tweet'ler, Facebook paylaşımları), resim (selfie), konum (gidilen yerler) ve zaman (sıklık ve zamanlama paylaşımı) gibi birey tarafından çevrim-içi olarak paylaşılan verilerin toplamıdır. Son olarak 'profesyonel kimlik' ise bireyin özellikle iş ve istihdamla ilişkili amaçlar için düzenlenmiş beceri kümesi, yetkinlikleri ve iş deneyimi anlamına gelir.[48] İnternet kullanıcılarının çoğu bu üç kimlik arasındaki etkileşimden, yani kendi özel dijital verilerinin işe alan kurumlar ve devletler tarafından nasıl kullanılabileceğinden habersizdir; ancak bu görünüşte ayrı olan veri türlerinin 'çapraz-toplanması' sadece kolay değildir, aynı zamanda ICT iş modeli bu şekilde yapılandırılmıştır. Ayrıca, gözetleme mekanizmalarının bireylerin kişisel yaşamlarına ve verilerine girebilmesini sağlayan bu üç kimlik türü arasındaki çapraz beslemedir. Örneğin kullanıcıların çoğu, (Twitter, Instagram, Amazon, Netflix gibi) farklı platformların her birinde farklı kullanıcı adlarına ya da kimlik bilgilerine sahip olsalar bile, devletlerin e-posta adreslerini izleyebileceklerinin farkında değildir. Kişisel bilgileri korumanın en kolay ve en bilinen yollarından bazıları parola güvenliği, çevrim-içi paylaşım ayarlarını kısıtlamak ve IP-engelleme araçları kullanmakla sınırlı olmakla birlikte, modern gözetlemenin mevcut durumu bunları kolayca aşabilmektedir. Bu nedenle mahremiyeti arttıran teknolojiler (PET'ler), gözetleme teknolojilerindeki ilerlemelere karşı yeni savunmalar geliştirerek çalışan ayrı bir sektördür ve kullanıcıların web trafiğini, belirli bir içeriği ya da bir web sitesi grubunu engelleyen ya da filtreleyen dijital bariyerleri baypas eden ya da yanlış yönlendiren bir şekilde maskeleyerek çalışmaktadır.[49] PET'ler iki ana kategoriye ayrılmaktadır: ağ tarafındaki PET'ler ve kullanıcı tarafındaki PET'ler. Ağ tarafındaki PET'ler, aşağıdakiler yoluyla kullanıcının web ile etkileşimini anonimleştirmeyi ve maskelemeyi amaçlar:

- kullanıcı bilgilerini, IP'sini ve konumunu vermeden engellenmiş ya da sansürlenmiş web sitelerine erişime olanak veren web tabanlı proxy'ler (vekiller) (örneğin kProxy, Whoer.net, Dontfilter ya da AnonyMouse)
- kullanıcının sunucuya bağlantısını karıştıran ve web-tabanlı proxy'lerin etkisini pekiştiren şifreli proxy'ler,
- kullanıcı trafiğini başka bir sunucu yoluyla başka yöne çevirerek bazı gözetleme araçlarını (ama tümünü değil) yanlış yönlendiren sanal özel ağlar (VPN'ler) (örneğin Hotspot Shield, Hamachi ya da Privoxy)
- ağ tarama trafiğini yönlendiren anonimlik ağları (örneğin Tor)
- uçtan uca şifreli mesajlaşma uygulamaları (örneğin Sig-

[45] Uluslararası Medeni ve Siyasi Haklar Sözleşmesi, Madde 17, BM Genel Kurulu kararı 68/167, BM İnsan Hakları Komitesi Genel Yorumları 27, 29, 31 ve 34.

[46] Yi Mou, Kevin Wu ve David Atkin, "Understanding the Use of Circumvention Tools to Bypass Online Censorship," New Media & Society 18, no. 5 (1 Mayıs 2016): 837–56, https://doi.org/10.1177/1461444814548994.

[47] Damon McCoy ve ark., "Shining Light in Dark Places: Understanding the Tor Network," in Privacy Enhancing Technologies, Lecture Notes in Computer Science (International Symposium on Privacy Enhancing Technologies Symposium, Springer, Berlin, Heidelberg, 2008), 63–76, https://doi.org/10.1007/978-3-540-70630-4_5.

[48] Liam Bullingham ve Ana C. Vasconcelos, "'The Presentation of Self in the Online World': Goffman and the Study of Online Identities," Journal of Information Science 39, no. 1 (1 Şubat 2013): 101–12, https://doi.org/10.1177/0165551512470051.

[49] Yang Wang, "Privacy-Enhancing Technologies," Handbook of Research on Social and Organizational Liabilities in Information Security, 2009, 203–27, https://doi.org/10.4018/978-1-60566-132-2.ch013.

nal ya da Telegram)
- kullanıcı bilgilerinin maskelenmesi amacıyla kimlik doğrulamaya, şifre çözmeye ve ön belleğe almaya olanak veren ters proxy'ler,
- özel olarak şifrelenmiş bir kanal yoluyla kullanıcı trafik verilerini 'tünelden geçiren' ve kullanıcı bilgilerini ifşa etmeden engellenmiş içeriğe erişim sağlayan Güvenli Kabuk Protokolü (SSH) tünelleme (örneğin PuTTY)

Öte yanda kullanıcı tarafındaki PET'ler, kullanıcı seviyesinde şifreleme, maskeleme ve yön değiştirme başlatan yazılım tabanlı uygulamalardır. Bunun bazı örnekleri arasında, kullanıcı tarayıcıya erişmeden önce ağ verilerini karıştıran Müşterek Giriş Arayüzü (CGI Proxy'ler) , ağ seviyesindeki gözetlemeyi baypas etmek için kendi aralarında doğrudan atlatma bağlantıları kuran HTTP proxy'leri ve güvenilen sunucular ve makineler arasındaki kullanıcı tarafı proxy'lerin tüm işlevlerini için kitle kaynak sağlayan p2p (eşler arası) sistemler yer almaktadır.[50] Bu araçlar, gözetim ve sansür altında yaşayan nüfusların büyük bölümünün söz konusu kontrollerin bazılarını atlatmasına olanak sağlamakla birlikte, gözetlemenin susturucu etkileri hala güçlüdür. İfade özgürlüğüne ve anonimliğe olanak veren araçların her zamankinden daha fazla kullanılabilir hale gelmelerine rağmen, bunlar özel hayatın gizliliğinin korunması için her zaman uygun değildir. En önemlisi, bir devlet bir ülkenin iletişim altyapısının tam kontrolünü ele geçirdiğinde, neredeyse tüm atlatma ve anonimlik araçlarını baypas edebilir ve şifreli platformlardaki etkileşimlerin ezici bir çoğunluğunu izleyebilir.

Teknik önlemlere ek olarak, devletlerin aşırı gözetleme önlemlerine karşı devam eden sivil toplum direniş hareketleri vardır. Bu gruplar altı ana kategoriye ayrılabilir: özel hayatın gizliliğine odaklanan hareketler, medeni haklar kuruluşları, insan hakları kuruluşları, tüketici koruma inisiyatifleri, dijital haklar aktivistleri ve ya belirli bir gözetleme teknolojisine (örneğin arka kapı kullanma) ya da bir bilgi türüne (örneğin kişisel veriler), korunmasız kişilere (örneğin Facebook kullanıcılar) ya da belirli bir iş sektörünün sıkıntılarına odaklanan 'tek konu inisiyatifleri'.[51] Örneğin Filipinler'de 2012'de çıkarılan bir yasa, emniyet makamlarına çevrim-içi bilgileri izlemeleri için önemli ölçüde genişletilmiş ve kontrol edilmeyen yetkiler vermiştir. Bu durum daha sonra aşırı bir sansür davranışına dönüşmüş, bu sayede kurumlar suç örgütlerinin yerine siyasi muhalefet gruplarına ait içeriği engellemeye ve sansürlemeye başlamıştır.[52] Bu nedenle ortaya çıkan halk protestoları, parlamentoya bilgi edinme özgürlüğünün korunması hakkında dilekçeler ve raporlar sunulması yoluyla ülkedeki İnternet mahremiyetinin ve dijital özgürlüklerin merkezi bir bileşeni haline gelen bir dijital haklar grubu olan FMA'nın (Medya Alternatifleri Vakfı) kurulmasına yol açmıştır.

AB'nin Ekim 2015'te Güvenli Liman anlaşmasını yürürlükten kaldırmasını sağlayan da çok sayıda Avrupalı dijital haklar grubunun ortak uyumlu çabaları olmuştur. Ardından Şubat 2017'de küresel sivil toplum grupları - Access Now, Bits of Freedom, Chaos Computer Club, Civil Liberties Union for Europe, Electronic Frontier Foundation, European Digital Rights, FITuG, Föreningen för Digitala Frioch Rättigheter Initiative für Netzfreiheit, IT-Political Association of Denmark, La Quadrature du Net, OpenMedia, Open Rights Group, Panoptykon Foundation, Son tus datos, Statewatch ve Vrijschrift – tarafında yazılan bir mektup, Avrupa Birliğinin Güvenli Liman Anlaşmasının yerini alan Privacy Shield veri transferi anlaşmasını askıya almayı değerlendirmesini sağlayan süreci başlatmıştır. Gelişmiş ülkeler arasındaki hızlanan gözetleme silahları yarışı (ABD ve Avrupa ülkeleri arasındaki ve AB içindeki dahil), küresel mahremiyete en sorunlu devlet müdahalelerinin bazılarına hep birlikte karşılık veren sıkı bir dijital haklar aktivistleri ağının ortaya çıkmasına yol açmıştır.[53] En sorunlu gelişmiş suistimallerin ABD'de meydana geldiği dikkate alındığında, American Civil Liberties Union, Stanford's Digital Civil Society Lab ve Digital Impact Lab gibi en sert dijital haklar gruplarının bazıları da bu ülkede ortaya çıkmıştır. Avrupa'da ise, European Privacy Association'ın yanı sıra, en önde gelen Avrupa dijital haklar inisiyatifleri için bir şemsiye kuruluş olan European Digital Rights (EDRi) bir diğer önemli oyuncudur. İsveç'te bulunan Pirate Party de dünya genelinde aktif bağlı taraflara sahip küresel bir dijital haklar aktivizm odağı haline gelmiştir.

Amerika Birleşik Devletlerindeki gözetleme-özel hayatın gizliliği tartışması, Kongre'nin - devletin Google ve AT&T hizmet sağlayıcılar yoluyla vatandaş verilerini izin gerekmeksizin

[50] Simone Fischer-Hbner ve Stefan Berthold, "Chapter 43 - Privacy-Enhancing Technologies1," in Computer and Information Security Handbook (Second Edition), ed. John R. Vacca (Boston: Morgan Kaufmann, 2013), 755–72, https://doi.org/10.1016/B978-0-12-394397-2.00043-X.

[51] Seeta Peña Gangadharan, "The Downside of Digital Inclusion: Expectations and Experiences of Privacy and Surveillance among Marginal Internet Users," New Media & Society 19, no. 4 (1 Nisan 2017): 597–615, https://doi.org/10.1177/1461444815614053.

[52] Jessamine Pacis, "State of Surveillance in the Philippines," Foundation for Media Alternatives (blog), 7 Nisan 2016, https://www.fma.ph/2016/04/07/state-of-surveillance-in-the-philippines/.

[53] Colin J. Bennett ve Charles D. Raab, The Governance of Privacy: Policy Instruments in Global Perspective (New York: Routledge, 2017).

toplamaya devam etmesini sağlayacak - FISA Değişiklikleri Yasasındaki Kısım 702'yi genişletmeyi tartıştığı 2018 başında en önemli anına ulaşmıştır.[54] Özgürlük odaklı yasa yapıcılardan oluşan iki partili bir grubun öncülüğünü yaptığı özel hayatın gizliliğini savunan taraf, devlet gözetiminin en aşırı yönlerinin bazılarını törpülemeyi hedeflerken, Temsilciler Meclisinin Cumhuriyetçi üyelerini ve istihbarat toplumunu içeren ve öncülüğünü Trump'ın yaptığı taraf, gözetleme kabiliyetlerinin sürekli olarak genişletilmesini istemektedir. Güçlü bir sivil toplum ağı tarafından desteklenen özel hayatın gizliliği savunucuları, FBI ve NSA'nın bir mahkeme emri olmadan e-postaları ve metin mesajlarını okumasını ve dijital mesajlaşma içeriklerini kitlesel olarak toplamasını sağlayan uygulamayı yasaklamaya çalışmaktadır. Öte yanda istihbarat toplumu, bu hamlenin Rusya ve Çin'in herhangi bir hukuki ya da siyasi denetim olmadan büyük ölçüde genişletilen gözetleme kabiliyetleri karşısında ABD'yi zayıf düşüreceğini öne sürmektedir. Sonuç olarak Kongre, ABD emniyet kurumlarının yabancı veri mahremiyeti kurallarına uymaksızın dünyanın herhangi bir yerinde depolanmış tüm verileri derlemelerine ve kaydetmelerine olanak veren bir diğer yasa olan CLOUD yasasını kabul etmiştir.[55] Ayrıca, ABD Başkanına, aynısını ABD'de depolanan veriler ile yapmaları için diğer uluslar ile özel anlaşmalar müzakere etme yetkisi vermektedir.

Gözetleme - Özel Hayatın Gizliliği Tartışması: Ana Pozisyonlara Bir Giriş

Gözetleme-özel hayatın gizliliği tartışmasının şu andaki durumu, politika bağlantıları ve politikaların birbirlerine etkisi ile hem iç hem de uluslararası politikaları eşit derecede ilgilendirmektedir. Ulusal düzeyde, tartışmanın devlet tarafı, gözetlemenin milli güvenlik stratejisinin ve terörle mücadele, uyuşturucuyla mücadele, kriminal fişleme ve diğer bileşenlerinin bir parçası olarak kullanılmasını savunmaktadır.[56] Özellikle artan terör tehdidi, aşırı sağ radikalleşme ve batı toplumlarında ortaya çıkan aşırı gruplar ile birlikte, gözetleme sadece siyasi olarak gerekli değil, aynı zamanda seçimler açısından halka hitap eden bir husus olarak görülmektedir.[57] Ancak tartışmanın toplum tarafı daha çok gözetlemenin boyutu ve kapsamı (gözetlemenin ne kadarı çok fazla) ve suistimalleri önlemek ve kamuoyunun rızasını almak için hangi hukuki ve yasama denetim mekanizmalarının kullanıldığı ile ilgilenmektedir. Öte yandan, İngiltere'deki gibi 'çifte kilitli' koruma mekanizmaları daha meşru olmalarına rağmen, bu tür modeller istihbaratın işlenmesini geciktirmekte ve kurumların - çoğu zaman kamuoyunu kızdıracak şekilde - önemli istihbaratları elden kaçırmalarına neden olmaktadır. Genellikle devletler, istihbaratın fiili bir saldırıya yol açacak şekilde geç işlenmesinin, halkın sevmediği ancak gerekli olan haşin gözetleme uygulamalarına kıyasla çok daha yüksek seçmen maliyetleri olduğuna inanmaktadır.[58]

Ancak bu ikilem ana akımda tartışıldığı kadar dolambaçsız değildir, çünkü tartışma devlet-toplum ilişkileri alanı ile sınırlı değildir. Tartışmadaki diğer paydaşlar, bilgi ve erişim için rekabet halinde olan yabancı istihbarat kurumları ve militan gruplardan bilgisayar korsanlarına kadar tehdit oluşturan devlet dışı aktörlerdir.[59] Kitlesel gözetleme, sadece terör gruplarına ve suç ağlarına karşı bir avantaj sağladığından değil, aynı zamanda tek bir istihbarat kurumunun gözetleme verilerine orantısız erişime sahip olmasını ve küresel bir 'dijital istihbarat tekeli' oluşturmasını da önlediğinden gerçekten küresel bir uygulama haline gelmektedir.[60] Bunun ardındaki mantık, tek bir istihbarat kurumunun diğer kurumlara kıyasla ezici ölçüde büyük hacimli verileri işleme ve depolama kabiliyetine sahip olmasının, söz konusu tekel konumundaki kuruma bu verileri diğer ülkelere karşı dijital casusluk ya da diplomatik sindirme biçiminde silah haline getirme olanağı verebileceği yolundadır. Bu nedenle diğer istihbarat kurum-

[54] Charlie Savage, "Surveillance and Privacy Debate Reaches Pivotal Moment in Congress," The New York Times, 10 Ocak 2018, sec. Politics, https://www.nytimes.com/2018/01/10/us/politics/nsa-surveillance-privacy-section-702-amendment.html.

[55] James Glanz, "Data Centers in Rural Washington State Gobble Power," The New York Times, 23 Eylül 2012, sec. Technology, https://www.nytimes.com/2012/09/24/technology/data-centers-in-rural-washington-state-gobble-power.html.

[56] David Cole ve Martin S. Lederman, "The National Security Agency's Domestic Spying Program: Framing the Debate Document," Indiana Law Journal 81 (2006): 1355–1426.

[57] Matthew A. Baum ve Tim Groeling, "Shot by the Messenger: Partisan Cues and Public Opinion Regarding National Security and War," Political Behavior 31, no. 2 (1 Haziran 2009): 157–86, https://doi.org/10.1007/s11109-008-9074-9.

[58] Jeffrey Monaghan ve Kevin Walby, "Making up 'Terror Identities': Security Intelligence, Canada's Integrated Threat Assessment Centre and Social Movement Suppression," Policing and Society 22, no. 2 (1 Haziran 2012): 133–51, https://doi.org/10.1080/10439463.2011.605131.

[59] Julian Richards, "Intelligence Dilemma? Contemporary Counter-Terrorism in a Liberal Democracy," Intelligence and National Security 27, no. 5 (1 Ekim 2012): 761–80, https://doi.org/10.1080/02684527.2012.708528.

[60] Angela Gendron, "Just War, Just Intelligence: An Ethical Framework for Foreign Espionage," International Journal of Intelligence and CounterIntelligence 18, no. 3 (1 Ekim 2005): 398–434, https://doi.org/10.1080/08850600590945399.

ları aynısını yapmak için kendi gözetleme kabiliyetlerini katlayarak arttırmakta ve dijital uzayda şeffaflık ve gizlilik açısından sonuçları olan tipik bir 'güvenlik ikilemi' yaratmaktadır. Çoğu devleti halkla dijital gözetlemeye ilişkin tartışmalara katılmaktan alıkoyan husus bu uluslararası istihbarat rekabeti konusudur.

Ancak kitlesel gözetlemenin özellikle demokratik rejimler için saklı maliyetleri vardır. Demokrasiler, halkın bir hükümetin politikalarını izleme, değerlendirme ve oy verme hakkına sahip olduğu bilgi şeffaflığı öncülü ile işler.[61] Demokrasinin mantığı, daha şeffaf ve daha iyi müzakere edilmiş politika yapma süreçlerinin yanlış hesaplama ya da yanlış algılama nedeniyle başarısız olma olasılığının, çok çeşitli görüşlerin söz konusu süreçlere dahil edilmesi sayesinde daha düşük olduğu şeklindedir. Ayrıca, halk ve temsilcileri hükümet uygulamaları konusunda daha fazla bilgiye ve bunlar üzerinde daha fazla denetime sahip olduklarından, demokratik hükümetlerin yolsuzlukları ve hataları örtbas etme ve istatistikleri manipüle etme olasılıkları da daha düşüktür, bu da hükümetlerin israfını önemli ölçüde azaltmaktadır.[62] Otoriter sistemler ise, ideoloji ya da kimlik temelinde farklı görüşlerin büyük bir kısmını politika yapma süreçlerinin dışında bıraktıkları ve yıldırdıkları için daha maliyetli savaşlara girmekte ve daha fazla batık maliyetler ile uğraşmaktadır, ayrıca bu sistemlerin komşuları ile uzun vadeli ihtilaflara düşmeleri olasılığı daha yüksektir. Ayrıca bu tür hükümetler 'milli güvenlik' gerekçesiyle anahtar politika, harcama ve atama bilgilerini halktan eksiksiz bir biçimde saklayabildiklerinden, insan ve malzeme kabiliyetlerinin yönetilmesi açısından daha savurgan olma eğilimi göstermektedir.

Ne demokrasiler ne de otoriter devletler, ne gözetlemeden ne de özel hayatın gizliliğinden tamamen vazgeçebilir. En şeffaf devletler bile, her zaman tam olarak yasal denetim ya da koruma mekanizmalarının kapsamında olmayan çok çeşitli gözetleme uygulamaları kullanabilir. Benzer şekilde, en otoriter ülkelerin bile, baskıların topyekun bir ayaklanmaya yol açmaması için görünüşte ifade özgürlüğünü ve özel hayatın gizliliğini korumaları gereklidir. Öte yandan demokrasilerin ve otoriter rejimlerin gözetleme doktrinlerini gerçekten birbirlerinden ayıran nokta, kamuoyunun rızası konusudur. Demokrasilerde halk, gözetleme yetkilerini suistimal eden ve devletin gizlilik aygıtını kötüye kullanan liderleri özgür ve adil seçimler yoluyla iktidardan indirebilir; bu, otoriter rejimlerdeki vatandaşların sahip olmadığı bir lükstür. Ayrıca demokrasilerde, vatandaşların hükümetlerini uzun vadede izlemelerine olanak veren bilgi edinme özgürlüğü yasaları, vatandaşlar ile siyasi gizlilik mekanizmaları arasında bir köprü görevi gören yasama komiteleri ve sürekli kamuoyu izlemesi için devlet gizlilik aygıtı içinde ve etrafında ağlar oluşturabilecek korunan özgür bir basın vardır.

Bu nedenle denetim mekanizmaları, özel hayatın gizliliği - gözetleme tartışmasının esas kilit taşıdır. Bu kurumlar hükümetlere yönelik koruma tedbirleri oluşturmak ve izlemek için tasarlanmıştır ve gözetleme/gizlilik politikalarına yönelik kamuoyu rızası için köprü görevi görürler.[64] Ayrıca hükümetin gizlilik tekelinin suistimal edilmesini seçmen maliyetleri ya da seçim davranışları yoluyla halk tarafından cezalandırılabilmesini sağlarlar. Ancak demokrasilerde gözetleme uygulamalarına karşı koruma tedbirleri oluşturma fikri, özellikle söz konusu demokrasiler ağır milli güvenlik krizleri ile karşı karşıya kaldıklarında çok sıkıntılı bir konuya dönüşebilir. Örneğin Kanada, İsveç, Norveç ve Hollanda, hükümetlerinin gözetleme yetkilerinin kapsamını sınırlayan çok güçlü koruma tedbirleri oluşturmuşlardır, oysa Amerika Birleşik Devletleri, Fransa, Yunanistan, İtalya ve İrlanda büyük ölçüde uğraştıkları çok çeşitli güvenlik sorunları nedeniyle bu tür tedbirler oluşturmamışlardır. Fransa'da, koruma tedbirlerinin olmaması Bataclan olayı sonrasındaki gözetleme yasalarına karşı geniş kapsamlı şüpheciliğe yol açmış ve askerlik hizmeti gerekliliklerine karşı direnişe neden olmuştur. Örneğin Amerika Birleşik Devletleri ve İngiltere'de, gözetleme kurumlarının aşırı hamleleri ve bunları kamuoyunun gözlerinden gizleme becerileri, bu geniş kapsamlı yetkilere karşı kurum içindeki muhalefeti ifade eden çok sayıda sızıntıya yol açmıştır.

Denetim; popülerliği, statüyü ve otoriteyi destekleyecek hızlı ve azami ödül getiren bir karar vermeye çalışan bir karar verici (ya da bir karar grubu) ile politika yapımı sırasında suistimalleri, aşırılığı ve hukuk dışı davranışları önlemeyi amaçlayan daha kapsamlı sivil toplum arasındaki bir rekabettir. Bu açıdan, yöneticiler denetimi her zaman, özellikle savaşlar,

61 Deibert Ronald J. ve Rohozinski Rafal, "Risking Security: Policies and Paradoxes of Cyberspace Security," International Political Sociology 4, no. 1 (7 Mart 2010): 15–32, https://doi.org/10.1111/j.1749-5687.2009.00088.x.

62 Colin J. Bennett ve David Lyon, eds., Playing the Identity Card: Surveillance, Security and Identification in Global Perspective, 1 basım (London ; New York: Routledge, 2008).

63 Wilson Matthew C. ve Piazza James A., "Autocracies and Terrorism: Conditioning Effects of Authoritarian Regime Type on Terrorist Attacks," American Journal of Political Science 57, no. 4 (3 Haziran 2013): 941–55, https://doi.org/10.1111/ajps.12028.

64 Siobhan Gorman, "Reengineering Surveillance Oversight," Lawfare, 6 Eylül 2017, https://www.lawfareblog.com/reengineering-surveillance-oversight.

protestolar ya da terör saldırıları gibi yüksek riskli ve zaman kısıtlı olaylar bakımından karar verme süreçlerini yavaşlatan gereksiz bir yük olarak görmektedir. Modern teknolojik gelişmeler gözetleme kurumları ile denetim mekanizmaları arasındaki yarışı adaletsiz bir yarış haline getirmektedir, çünkü gözetleme kurumları bu yarışta açık bir avantaja sahiptir. Gelişmiş teknolojik kabiliyetlere sahip kurumlar, gözetleme uygulamalarının karmaşık ayrıntılarını ve gizledikleri sırların miktarını çok daha iyi saklamakta ve denetim mekanizmalarının zamanla geri gitmelerine ve yavaşlamalarına neden olmaktadır. İngiltere gibi bir demokraside dahi, bilgi edinme özgürlüğü yasasının zayıflığı ve denetim mekanizmalarının yavaşlığı hem halkın hem de Başbakanlığa bağlı İstihbarat Güvenliği Komitesinin (Intelligence Security Committee - ISC) GCHQ gözetleme uygulamalarının kapsamını ve derinliğini tam olarak anlamalarını önlemektedir; bu sorun ABD'de daha büyük boyuttadır.[65]

Son bir kaç yıl içinde Kanada, Belçika, Hırvatistan, Norveç, İsveç ve Hollanda, ulusal resmi güvenlik komitelerinin yanı sıra uzman, sivillerin öncülük ettiği denetim organları oluşturma konusunda önemli ilerlemeler sağlamışlardır.[66] Bu bağımsız organların Avrupalı örneklerinin çoğu seçilmemiş, halktan uzmanlardan oluşmakla birlikte, İsveç ve Kanada teknik sivil uzmanların yasa yapıcılar ile birlikte görev yaptığı melez bağımsız bir komite oluşturmuşlardır. Bu bağımsız kurumların faydası, teknik açıdan yetkin olmayan ve tamamen yasama üyelerinden oluşan komitelerden ziyade, teknik ayrıntıların yasa yapıcıların kendilerine daha hızlı bir şekilde sunulmasıdır. Yararlı ancak eski bir standart, gözetleme raporlarının tümünü İngilizceye tercüme eden ve denetim verilerinin tümünü diğer ülkelerin ve Belçika vatandaşlarının kullanımı için çevrim-içi olarak yayınlayan Belçika Daimi İstihbarat İnceleme Komitesi tarafından belirlenmiştir.[67] Komite, gözetlemenin ancak yasama organları arasındaki uluslararası bir işbirliği mekanizması ile çözülebilecek uluslar ötesi bir sorun olduğuna inandığından, söz konusu veriler halka açıklanmış ve İngilizceye tercüme edilmiştir.

Bununla birlikte, tıpkı özgür ve adil seçimlerin denetimin ve bilgi edinme özgürlüğünün var olması sayesinde anlam kazandığı gibi, bunun tersi de doğrudur: denetim mekanizmaları, ancak seçimler gerçekten rekabete açık ve özgür olduğunda işe yarayabilir. Mevcut küresel akımlar, hoşgörüsüz eğilimler üreten demokrasilerin seçim hilelerine ya da üstü kapalı tehditler kullanmaya gittikçe daha bağımlı hale geldiği sorunlu bir seçim ortamı ortaya çıkarmaktadır. Dijital gözetleme denetimi de dahil olmak üzere herhangi bir denetim türünün işe yarayabilmesi için, ülkelerin anlamlı seçim ve bilgi mekanizmalarına sahip olmaları gereklidir, böylece halk hükümetleri eksiksiz bir biçimde izleyebilir ve suistimal hallerinde hükümetleri (ya seçimlerde ya da seçmen maliyetleri yoluyla) cezalandırabilir.

Sonuç: Gözetleme karşı Özel Hayatın Gizliliği - Ne Kadarı Çok Fazla?

Toplum, karar vericilerin gizliliği ve gözetlemeyi yolsuzlukları, kötü yönetimi ve yanlış kararları saklamak yerine milli güvenliği desteklemek için kullanacağından nasıl emin olabilir? Demokratik devletler, mevcut gözetleme rejiminin rakip devletlere karşı ülkenin stratejik avantajının koruması ile toplumun siyasi süreçler hakkında bilgi alma hakkı arasındaki en iyi orta nokta olduğunu halka nasıl iletebilir? Bir terörle mücadele yetkilisi, belirli bir gözetleme taktiğinin terör eylemlerinin meydana gelmesini azalttığını ve dolayısıyla programın meşruluğunu arttırdığını, hedeflenen aşırı gruba ulaşma yöntemini ya da yolunu açığa vurmadan topluma nasıl anlatabilir? Halk ve/veya parlamento, terörle mücadele yetkilisi gözetleme programının başarısını ortaya koyduğunda, söz konusu yetkilinin programın hatalarını ve suistimallerini gizlemek için verileri seçerek kullanmadığından nasıl emin olabilir?

Bu soruların yanıtları sadece zor değil, aynı zamanda bir ülkenin güvenlik, kurumsal, yönetim ve örgütsel kültürü bakımından kültürel niteliktedir. Bazı demokratik ülkelerde artan gizlilik yolsuzluğun ve kötü yönetimin saklanması olarak görülebilmekle birlikte, doğrudan güvenlik tehditleri (sınır aşırı ya da terörist) ile karşı karşıya olan başka ülkeler bu gizliliği gerekli olarak görebilir. Örneğin Bataclan olayından sonraki Fransız gözetleme uygulamaları seçmenler tarafından aşırı olarak değerlendirmiş ve programın lehine ikna edici bir savunma yapabilecek siyasetçiler ve emniyet yetkileri olmadığından kamuoyu desteği gittikçe azalmıştı. Seçmenler askerlik hizmetinin uzatılmasına ya da yabancı operasyonlarda

65 Hayley Evans, "Summary: U.K. Intelligence and Security Committee Annual Report," Lawfare, 4 Ocak 2018, https://www.lawfareblog.com/summary-uk-intelligence-and-security-committee-annual-report.

66 Zachary K. Goldman ve Samuel J. Rascoff, Global Intelligence Oversight: Governing Security in the Twenty-First Century (Oxford: Oxford University Press, 2016).

67 Nicolas Boring, "Foreign Intelligence Gathering Laws: Belgium," Web sayfası, Haziran 2016, https://www.loc.gov/law/help/intelligence-activities/belguim.php.

kullanılacak ağır toplar satın alınmasına direnerek hükümeti cezalandırdığından, söz konusu azalmanın doğrudan yansımaları olmuştu. İstihbarat faydalı olmakla birlikte, önemli bir çatışma için kaynakların seferber edilmesini ya da müttefiklerin desteklenmesine yönelik lehte kamuoyu oluşturulmasını kendi başına sağlayamaz: kamuoyunun rızasını hükümetlerin kazanması gereklidir.

Bir demokrasi için en kötü uygulama, hesap verebilirlik mekanizmalarını kurmadan bilgi, istihbarat ve milli güvenlik kararlarının küçük bir karar vericiler grubunun elinde olacak şekilde aşırı merkezileştirilmesi gibi görünmektedir. Bu, temel politika konularında uzun vadeli şüpheler oluşturur, bu tür siyasi önermelere karşı kalıcı kamuoyu direncine yol açar ve - söz konusu sesler ana akımda kendilerine yer bulamadığında bile - ülkenin dış politika çabalarını baltalar. İşkence ya da sivil ölümleri gibi hukuk dışı çatışma uygulamaları meydana geldikten sonra sızıntılar sonucunda ifşa edildiğinde bu tür direnişler önemli ölçüde artacaktır.

Öte yandan iyi demokratik uygulamalar bir derece denetim ve koruma tedbirlerini içerir, ancak bunlar ne kadar olmalıdır? Michael Colaresi, bir 'zaman aralığı' modelini savunmaktadır.[68] Zaman aralığı modelinde, devlet kamuoyunun rızasını gerektiren politikayı, söz konusu politikanın o andaki gizliliğini korumak için zaman içinde aşamalı olarak açıklar, ama ardından makul bir zaman çerçevesi içinde bu politikayı halkın tartışmasına ve rızasına açar. Genellikle, özel hayatın gizliliği-gözetleme tartışmasındaki temel tartışmalardan birini oluşturan husus, uzun bir süre (bazen süresiz) gizli kalan sırlardır. İkincisi, 'geriye dönük hesap verebilirlik' mekanizmalarının oluşturulması gereklidir, böylece ulusal gizliliği suistimal edenler bir noktada söz konusu aşırılığın sonuçları ile karşı karşıya kalacaktır. Bunu yapabilmek için, güvenilir bir arşiv altyapısının yanı sıra gizlenen belgelerin ya da kanıtların çoğunu halka sunmak için zaman içinde güvenilir bir biçimde geriye gidebilecek kurumsal süreçlerin mevcut olması gereklidir. Yasama ve hukuk denetimi yeterince güçlü olmalıdır, böylece gizliliğin zaman aralığı sona erdiğinde, her iki kurum yürütmenin gizlilik altında neler yapmış olduğunu makul bir şekilde değerlendirebilir. Demokrasiler her zaman acil durumlar sırasında gizliliğin kullanımını koruyan ve denetleyen ve liderlere geç de olsa mutlak bir şekilde bedel ödeten güçlü kurumlara sahiptir.

Otokrasilerde bu tür mekanizmalar mevcut değildir ve ne yasama denetimi ne de hukuk denetimi seçenekleri, zaman aralığının sona ermesinden uzun süre sonra bile aşırılığa kaçan yöneticilere hatasız bir şekilde herhangi bir sorumluluk yükleyebilir. Bu senaryo otokrat liderler için iyi bir senaryo gibi görünmekle birlikte, politikalara yönelik kamuoyu desteğinin daha fazla temsile dayanan koşullardaki destekten her zaman daha az olduğu yalnızlık içeren bir senaryodur, ayrıca sadece siyasi olarak atanan kimselerin girebildiği karar verici grup açısından da yalnızlık içermektedir. Savaş, sivil itaatsizlik ya da deniz aşırı askeri harekatlara katılma gibi kriz senaryolarında, liderler söz konusu acil durumda iyi bir performans sergilemek için büyük miktarlarda milli kaynağı (parasal, teknolojik, insan gücü ve insan niteliği) seferber etmek zorunda kalırlar. Bu konularda verilen kararlar, yerel ve uluslararası kitleler için eşit ölçüde kalın bir gizem tabakası ile örtüldüğünde, süreç söz konusu milli kaynakların büyük bölümlerini ihmal eder ve lideri hızlı ve üniter ama ülke için yeterli olmayan kararlar vermeye zorlar. Ayrıca, toplum devletin neden haşin dijital gözetleme önlemleri kullandığı ve sivillere yönelik aktif gözetim uyguladığı konusunda ikna olmadığında, direniş daha da güçlenir.

Sonuç olarak, demokrasilerin ülkenin siyasi kültürüne, ancak aynı zamanda evrensel insan haklarına uyan bir gözetleme-özel hayatın gizliliği dengesi kurmaları gereklidir. Bu bağlamda denetim görevi ağır bir görevdir: suistimalleri ve aşırılıkları tespit etmek için yürütme ve istihbarat toplumunu sürekli olarak takip etmesi ve aynı zamanda teknolojik açıdan yetkin kalması gerekmektedir. Denetim mekanizmalarının işe yaramadığı zamanların çoğunda bunun nedeni söz konusu mekanizmaların teknik olarak eskimiş olmaları ya da gözetlemenin ve izlemenin yapıldığı daha yeni teknolojileri anlayamamalarıdır. Dijital gözetleme denetimi, gücü en üst düzeye çıkaracak davranışlara girmek isteyen fevri bir yönetici ile yolsuzluğu, kötü yönetimi ve suistimalleri önlemekle ilgilenen araştırmacı bir halk arasında denge kurmak zorundadır. Yürütme ile emniyet-istihbarat toplumları doğal olarak denetimden kaçınmak isteyecek ve halk, devletlerin güvenlik ikilemi sorunları dikkate alındığında gerçekçi olmayan maksimalist bir şeffaflık anlayışına sahip olacaktır. Denetim mekanizmaları, gözetleme-özel hayatın gizliliği alanındaki teknolojik gelişmelerin gerisinde kalırlarsa ya da gizlilik sürecini izlemeleri çok uzun sürerse, bir denge kurmada başarısız olacaklardır. Yani, tıpkı çevrim-dışı demokraside olduğu gibi, çevrim-içi demokrasi de ancak denetim mekanizmaları ve koruyucuları kadar güçlüdür.

[68] Colaresi;, Democracy Declassified.

Referanslar

Altheide, David L. "The Triumph of Fear: Connecting the Dots about Whistleblowers and Surveillance." *International Journal of Cyber Warfare and Terrorism (IJCWT)* 4, no. 1 (1 Ocak 2014): 1–7. https://doi.org/10.4018/ijcwt.2014010101.

Ball, Kirstie, and Laureen Snider. *The Surveillance-Industrial Complex: A Political Economy of Surveillance.* New York: Routledge, 2013.

Baum, Matthew A., and Tim Groeling. "Shot by the Messenger: Partisan Cues and Public Opinion Regarding National Security and War." *Political Behavior* 31, no. 2 (1 Haziran 2009): 157–86. https://doi.org/10.1007/s11109-008-9074-9.

BBC/Panorama, Source: "Edward Snowden: GCHQ Wants to Own Your Phone – Video." *The Guardian*, 5 Ekim 2015, sec. US news. http://www.theguardian.com/us-news/video/2015/oct/05/edward-snowden-gchq-wants-own-your-phone-video.

Bennett, Colin J., and David Lyon, eds. *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective.* 1 basım. London ; New York: Routledge, 2008.

Bennett, Colin J., and Charles D. Raab. *The Governance of Privacy: Policy Instruments in Global Perspective.* New York: Routledge, 2017.

Bentham, Jeremy. *Panopticon: The Inspection House.*CreateSpace Independent Publishing Platform, 2017.

Blum, Stephanie Cooper. "What Really Is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform." *Boston University Public Interest Law Journal* 18 (2009 2008): 269–314.

Boring, Nicolas. "Foreign Intelligence Gathering Laws: Belguim." Web sayfası, Haziran 2016. https://www.loc.gov/law/help/intelligence-activities/belguim.php.

———. "Foreign Intelligence Gathering Laws: France | Law Library of Congress." Web sayfası, Aralık 2014. https://www.loc.gov/law/help/foreign-intelligence-gathering/france.php.

Born, Dr Hans, and Ms Marina Caparini. *Democratic Control of Intelligence Services: Containing Rogue Elephants.* Ashgate Publishing, Ltd., 2013.

Botsman, Rachel. "Big Data Meets Big Brother as China Moves to Rate Its Citizens." WIRED UK, Ekim 2017. http://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion.

Bullingham, Liam, and Ana C. Vasconcelos. "'The Presentation of Self in the Online World': Goffman and the Study of Online Identities." *Journal of Information Science* 39, no. 1 (1 Şubat 2013): 101–12. https://doi.org/10.1177/0165551512470051.

Carey, Scott. "Investigatory Powers Act: What You Need to Know." ComputerworldUK, Ocak 2018. https://www.computerworlduk.com/security/draft-investigatory-powers-bill-what-you-need-know-3629116/.

Chadwick, Andrew, and Philip N. Howard. *Routledge Handbook of Internet Politics.* Taylor & Francis, 2010.

Chang, Alvin. "The Facebook and Cambridge Analytica Scandal, Explained with a Simple Diagram." Vox, 23 Mart 2018. https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram.

"China Passes Tough New Intelligence Law." *Reuters*, 28 Haziran 2017. https://www.reuters.com/article/us-china-security-lawmaking/china-passes-tough-new-intelligence-law-idUSKBN19I1FW.

Colaresi;, Michael P. *Democracy Declassified: The Secrecy Dilemma in National Security by Michael P. Colaresi.* Oxford University Press, 2014.

Cole, David, and Martin S. Lederman. "The National Security Agency's Domestic Spying Program: Framing the Debate Document." *Indiana Law Journal* 81 (2006): 1355–1426.

Davis, Robert N. "Striking the Balance: National Security vs. Civil Liberties." *Brooklyn Journal of International Law* 29 (2004 2003): 175–238.

De Capitani Di Vimercati, Sabrina, Sara Foresti, Giovanni Livraga, and Pierangela Samarati. "Data Privacy: Definitions and Techniques." *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 20, no. 6 (1 Aralık 2012): 793–817. https://doi.org/10.1142/S0218488512400247.

Deibert Ronald J., and Rohozinski Rafal. "Risking Security: Policies and Paradoxes of Cyberspace Security." *International Political Sociology* 4, no. 1 (7 Mart 2010): 15–32. https://doi.org/10.1111/j.1749-5687.2009.00088.x.

Donohue, Laura K. *The Future of Foreign Intelligence: Privacy and Surveillance in a Digital Age*. Oxford: Oxford University Press, 2016.

Evans, Hayley. "Summary: U.K. Intelligence and Security Committee Annual Report." Lawfare, 4 Ocak 2018. https://www.lawfareblog.com/summary-uk-intelligence-and-security-committee-annual-report.

Fischer-Hbner, Simone ve Stefan Berthold. "Chapter 43 - Privacy-Enhancing Technologies1." *In Computer and Information Security Handbook (Second Edition)*, editör John R. Vacca, 755–72. Boston: Morgan Kaufmann, 2013. https://doi.org/10.1016/B978-0-12-394397-2.00043-X.

Foucault, Michel. *Discipline & Punish: The Birth of the Prison*. Çeviren Alan Sheridan. New York: Vintage Books, 1995.

Gangadharan, Seeta Peña. "The Downside of Digital Inclusion: Expectations and Experiences of Privacy and Surveillance among Marginal Internet Users." New Media & Society 19, no. 4 (1 Nisan 2017): 597–615. https://doi.org/10.1177/1461444815614053.

Gendron, Angela. "Just War, Just Intelligence: An Ethical Framework for Foreign Espionage." *International Journal of Intelligence and CounterIntelligence* 18, no. 3 (1 Ekim 2005): 398–434. https://doi.org/10.1080/08850600590945399.

Gesley, Jenny. "Foreign Intelligence Gathering Laws: Germany." Web sayfası, Haziran 2016. https://www.loc.gov/law/help/intelligence-activities/germany.php.

Gibbs, Samuel. "What Is 'Safe Harbour' and Why Did the EUCJ Just Declare It Invalid?" the Guardian, 6 Ekim 2015. http://www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection.

Glanz, James. "Data Centers in Rural Washington State Gobble Power." *The New York Times*, 23 Eylül 2012, sec. Technology. https://www.nytimes.com/2012/09/24/technology/data-centers-in-rural-washington-state-gobble-power.html.

Goad, Ben. "New Pressure on US Tech to Comply with China's Access Demands." Text. TheHill, 16 Ekim 2015. http://thehill.com/policy/cybersecurity/257194-new-pressure-on-us-tech-to-comply-with-chinas-access-demands.

Goldman, Zachary K., and Samuel J. Rascoff. *Global Intelligence Oversight: Governing Security in the Twenty-First Century*. Oxford: Oxford University Press, 2016.

Gorman, Siobhan. "Reengineering Surveillance Oversight." Lawfare, 6 Eylül 2017. https://www.lawfareblog.com/reengineering-surveillance-oversight.

Greenwald, Glenn, and Spencer Ackerman. "How the NSA Is Still Harvesting Your Online Data." the Guardian, 27 Haziran 2013. http://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection.

"Hacker Lexicon: What Is a Backdoor?" WIRED. 28 Mart 2018'de erişilmiştir. https://www.wired.com/2014/12/hacker-lexicon-backdoor/.

Hern, Alex. "Strava Suggests Military Users 'Opt Out' of Heatmap as Row Deepens." the Guardian, 29 Ocak 2018. http://www.theguardian.com/technology/2018/jan/29/strava-secret-army-base-locations-heatmap-public-users-military-ban.

Himmelfarb, Gertrude. *The Roads to Modernity: The British, French, and American Enlightenments*. Yeni basım. New York New York: Vintage, 2005.

Landau, S. "Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations." *IEEE Security Privacy* 11, no. 4 (Temmuz 2013): 54–63. https://doi.org/10.1109/MSP.2013.90.

Langner, R. "Stuxnet: Dissecting a Cyberwarfare Weapon." *IEEE Security Privacy* 9, no. 3 (Mayıs 2011): 49–51. https://doi.org/10.1109/MSP.2011.67.

Lee, Dave. "China and US Clash over Backdoors." *BBC News*, 4 Mart 2015, sec. Technology. http://www.bbc.com/news/technology-31729305.

Ling, Justin. "The Story of How Canadian Police Committed Arson to Stop a Black Panther Meeting." VICE News, Haziran 2017. https://news.vice.com/en_ca/article/eva8da/story-of-how-canadian-police-committed-arson-to-stop-a-black-panther-meeting.

Luhn, Alec. "Russia Passes 'Big Brother' Anti-Terror Laws." the Guardian, 26 Haziran 2016. http://www.theguardian.com/world/2016/jun/26/russia-passes-big-brother-anti-terror-laws.

Lütticke, Marcus. "New Leaks Show Germany's Collusion with NSA | DW | 21.06.2014." DW.COM, Haziran 2014. http://www.dw.com/en/new-leaks-show-germanys-collusion-with-nsa/a-17726141.

Lyon, David, Kirstie Ball, and Kevin D. Haggerty. *Routledge Handbook of Surveillance Studies*. New York: Routledge, 2012.

MacAskill, Ewen, Julian Borger, Nick Hopkins, Nick Davies, and James Ball. "GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications." the Guardian, 21 Haziran 2013. http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

Marx Gary T. "A Tack in the Shoe: Neutralizing and Resisting the New Surveillance." *Journal of Social Issues* 59, no. 2 (29 Nisan 2003): 369–90. https://doi.org/10.1111/1540-4560.00069.

McCoy, Damon, Kevin Bauer, Dirk Grunwald, Tadayoshi Kohno, and Douglas Sicker. "Shining Light in Dark Places: Understanding the Tor Network." *In Privacy Enhancing Technologies*, 63–76. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg, 2008. https://doi.org/10.1007/978-3-540-70630-4_5.

Meister, Andre. "How the German Foreign Intelligence Agency BND tapped the Internet Exchange Point DE-CIX in Frankfurt, since 2009." *netzpolitik.org* (blog), 31 Mart 2015. https://netzpolitik.org/2015/how-the-german-foreign-intelligence-agency-bnd-tapped-the-internet-exchange-point-de-cix-in-frankfurt-since-2009/.

Miller, Jacques-Alain ve Richard Miller. "Jeremy Bentham's Panoptic Device." *Ekim* 41 (1987): 3–29. https://doi.org/10.2307/778327.

Mitchell, Anna, and Larry Diamond. "China's Surveillance State Should Scare Everyone." *The Atlantic*, 2 Şubat 2018. https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/.

Monaghan, Jeffrey ve Kevin Walby. "Making up 'Terror Identities': Security Intelligence, Canada's Integrated Threat Assessment Centre and Social Movement Suppression." *Policing and Society* 22, no. 2 (1 Haziran 2012): 133–51. https://doi.org/10.1080/10439463.2011.605131.

Mou, Yi, Kevin Wu ve David Atkin. "Understanding the Use of Circumvention Tools to Bypass Online Censorship." *New Media & Society* 18, no. 5 (1 Mayıs 2016): 837–56. https://doi.org/10.1177/1461444814548994.

Pacis, Jessamine. "State of Surveillance in the Philippines." *Foundation for Media Alternatives* (blog), 7 Nisan 2016. https://www.fma.ph/2016/04/07/state-of-surveillance-in-the-philippines/.

Phillips, Tom. "China Testing Facial-Recognition Surveillance System in Xinjiang – Report." the Guardian, 18 Ocak 2018. http://www.theguardian.com/world/2018/jan/18/china-testing-facial-recognition-surveillance-system-in-xinjiang-report.

Privacy International. "A New Era of Mass Surveillance Is Emerging Across Europe." *Medium* (blog), 17 Ocak 2017. https://medium.com/privacy-international/a-new-era-of-mass-surveillance-is-emerging-across-europe-3d56ea35c48d.

Richards, Julian. "Intelligence Dilemma? Contemporary Counter-Terrorism in a Liberal Democracy." *Intelligence and National Security* 27, no. 5 (1 Ekim 2012): 761–80. https://doi.org/10.1080/02684527.2012.708528.

Rosen, Jeffrey. "The Right to Be Forgotten Symposium Issue: The Privacy Paradox: Privacy and Its Conflicting Values." *Stanford Law Review Online* 64 (2012 2011): 88–92.

Savage, Charlie. "Surveillance and Privacy Debate Reaches Pivotal Moment in Congress." *The New York Times*, 10 Ocak 2018, sec. Politics. https://www.nytimes.com/2018/01/10/us/politics/nsa-surveillance-privacy-section-702-amendment.html.

Soldatov, Andrei ve Irina Borogan. "Inside the Red Web: Russia's Back Door onto the Internet – Extract." the Guardian, 8 Eylül 2015. http://www.theguardian.com/world/2015/sep/08/red-web-book-russia-internet.

Wang, Yang. "Privacy-Enhancing Technologies." *Handbook of Research on Social and Organizational Liabilities in Information Security*, 2009, 203–27. https://doi.org/10.4018/978-1-60566-132-2.ch013.

Willsher, Kim. "France Approves 'Big Brother' Surveillance Powers despite UN Concern." the Guardian, 24 Temmuz 2015. http://www.theguardian.com/world/2015/jul/24/france-big-brother-surveillance-powers.

Wilson Matthew C. ve Piazza James A. "Autocracies and Terrorism: Conditioning Effects of Authoritarian Regime Type on Terrorist Attacks." *American Journal of Political Science* 57, no. 4 (3 Haziran 2013): 941–55. https://doi.org/10.1111/ajps.12028.

Wong, Cynthia. "Big Brother Is Watching: Why We Should Fear Surveillance in the New World Order." Newsweek, 7 Şubat 2017. http://www.newsweek.com/state-surveillance-europe-populism-cctv-citizens-553857.

Ekonomi ve Dış Politika Araştırmalar Merkezi

edam

Siber Politikalar ve Dijital Demokrasi 2018/4

Mayıs 2018

Dijital Gözetleme, Milli Güvenlik ve Özel Hayatın Gizliliği Siyaseti

H. Akın Ünver | EDAM, Oxford CTGA & Kadir Has Üniversitesi